D19

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel und H. Hasse

Band 171

Heft 1

Ausgegeben den 30. April 1934

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1934

Band 171. Heft 1.

Inhaltsverzeichnis.

Seite

van der Waerden, B. L., Elementarer Beweis eines zahlentheoretischen Existenztheorems 1

Witt, Ernst, Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper 4

Iyanaga, S., Zur Theorie der Geschlechtermoduln 12

Scholz, A. und **O. Taussky,** Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm 19

Oehlert, M., Über die Definition der Zeuthen-Segreschen Invariante 42

Rédei, L., Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. . . . 55

Rédei, L., Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper 61

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgendeinem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse:
An die Redaktion des Journals für die reine und angewandte Mathematik
Professor Dr. Kurt Hensel, Marburg-Lahn, Behringweg 7.

Elementarer Beweis eines zahlentheoretischen Existenztheorems.

Von *B. L. van der Waerden* in Leipzig.

H. Hasse hat seiner arithmetischen Theorie der Algebrenklassen [1]) ein Existenztheorem (0.3) zugrunde gelegt, welches einige Ähnlichkeit mit dem Artinschen Hilfssatz zum allgemeinen Reziprozitätsgesetz [2]) besitzt und auch an dessen Stelle zum Beweis des Reziprozitätstheorems benutzt werden kann. Er spricht a. a. O. die Vermutung aus, daß man dieses Existenztheorem elementar müsse beweisen können, sofern man sich nicht darauf kapriziert, die verlangte Klasseneinteilung durch einen Primzahlmodul zu realisieren. Diese Vermutung stellt sich nun als richtig heraus.

Der Spezialfall $r = 1$ des Existenzsatzes, der übrigens zum Beweis des Reziprozitätsgesetzes hinreicht, heißt so: *Es gibt bei gegebenen natürlichen Zahlen $a > 1$ und k stets eine zyklische Kongruenzklasseneinteilung der rationalen Zahlen, in welcher der Exponent von a durch k teilbar wird.*

Diesen Spezialfall hat Chevalley in seiner soeben publizierten Thèse [3]) elementar bewiesen; seinen Beweis hat H. Hasse in seiner hektographierten Vorlesung „Klassenkörpertheorie“ unter Benutzung von Sätzen von Vandiver und Birkhoff noch weiter vereinfacht. Wir werden die Hassesche Fassung des Beweises unten (Satz 1) mitteilen. Auf diesen Spezialfall gründet sich dann der allgemeine Satz (Satz 3).

Unser Beweis beruht auf folgendem Gedankengang. Gegeben sind die Zahlen $a_1, \ldots, a_r$ und ein Exponent k, den wir zunächst als Primzahlpotenz l^ν annehmen. Auf Grund des Spezialfalles gibt es zu den einzelnen a_λ Klasseneinteilungen, in denen ihre Exponenten durch l^ν teilbar werden. Die Durchkreuzung dieser zyklischen Klasseneinteilungen ergibt eine nicht zyklische Klasseneinteilung. Diese besitzt aber eine zyklische Vergröberung, in welcher die Exponenten aller a_λ durch l^ν teilbar sind (Satz 2). Der Übergang von $k = l^\nu$ zu beliebigem k (Satz 3) bereitet dann keine Schwierigkeiten mehr.

Die zyklischen Klasseneinteilungen werden am bequemsten durch Charaktere definiert [4]). Die Werte dieser Charaktere braucht man nicht als komplexe Einheitswurzeln aufzufassen, sondern man kann sie als Elemente irgendeiner abstrakten zyklischen Gruppe der Ordnung h deuten, wo h das K. G. V. aller vorkommenden Klassengruppenordnungen ist.

---

[1]) H. Hasse, Die Struktur der R. Brauerschen Algebrenklassengruppe, Math. Ann. **107** (1933), S. 731.

[2]) E. Artin, Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Hamburg **5** (1927), S. 353.

[3]) C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Faculty Sci. Univ. Tokyo II (1933), S. 365—476.

[4]) Darauf, daß diese Art der Definition übersichtlicher ist als meine ursprüngliche, welche eine Art „additiver Charaktere“ benutzte, machte mich Herr Hasse in freundlicher Weise aufmerksam.

Im folgenden bezeichnen $l, p, \ldots$ Primzahlen, $a, b, \ldots, x, y, \lambda, \mu, \nu, \ldots$ natürliche Zahlen. Die mit a (bzw. $a_\lambda, a_\varkappa$) bezeichneten Zahlen sind immer > 1.

Hilfssatz [5]). *Ein Primteiler p von*

$$Q = \frac{a^{l^\nu+1} - 1}{a^{l^\nu} - 1}$$

ist niemals zugleich Teiler des Nenners $a^{l^\nu} - 1$, ausgenommen eventuell für $p = l$. Die Primzahl l geht in Q höchstens zur ersten Potenz auf.

Beweis. Setzt man $a^{l^\nu} - 1 = b$, so ist

$$(1) \quad Q = \frac{(b+1)^l - 1}{b} = b^{l-1} + \binom{l}{1} b^{l-2} + \cdots + \binom{l}{l-2} b + \binom{l}{l-1}.$$

Aus $p|Q$ und $p|b$ folgt demnach $p\left|\binom{l}{l-1}\right.$, also $p = l$. Ist aber $p = l$ ein Teiler von Q, so folgt aus (1) $l|b^{l-1}$, also $l|b$, also für $l > 2$ wieder nach (1) $Q \equiv l \pmod{l^2}$. Für $l = 2$ und $l|Q$ ist a ungerade, also $b = a^{2^\nu} - 1 \equiv 0 \pmod 4$, also wieder nach (1) $Q \equiv l \pmod{l^2}$.

Satz 1. *Es gibt bei gegebenen a, l, ν eine Primzahl p mit den Eigenschaften*

$$a^{l^\nu+1} \equiv 1 \pmod p, \qquad a^{l^\nu} \not\equiv 1 \pmod p.$$

Beweis. Nach dem Hilfssatz ist die dort definierte Zahl Q höchstens durch l^1 teilbar, aber nach (1) $Q > l$; also hat Q mindestens einen von l verschiedenen Primteiler p. Dieser hat nach dem Hilfssatz alle verlangten Eigenschaften.

Bemerkung. Satz und Hilfssatz gelten, falls l ungerade ist, auch für $\nu = 0$.

Satz 2. *Es gibt bei gegebenen $a_1, a_2, \ldots, a_r, \nu, l$ eine zyklische Kongruenzklasseneinteilung der rationalen Zahlen, bei der die Exponenten von $a_1, \ldots, a_r$ durch $l^{\nu+1}$ teilbar sind.*

Beweis. Man wähle ω so groß, daß erstens $l^\omega > r$, zweitens $l^{\nu+\omega}$ alle Exponenten der Zahlen a_λ modulo den in $a_1 a_2 \cdots a_r$ aufgehenden Primzahlen übertrifft. Es gibt dann nach Satz 1 zu jedem a_λ eine solche (nicht in $a_1 a_2 \cdots a_r$ aufgehende) Primzahl p_λ, daß

$$(2) \qquad a_\lambda^{l^{\nu+\omega}} \equiv 1 \pmod{p_\lambda}, \qquad a_\lambda^{l^{\nu+\omega-1}} \not\equiv 1 \pmod{p_\lambda}.$$

Ist dann $\chi_\lambda(x)$ ein solcher Charakter mod p_λ, dessen Ordnung genau die in $p_\lambda - 1$ aufgehende Potenz l^{μ_λ} ist, so hat $\chi_\lambda(a_\lambda)$ genau die Ordnung $l^{\nu+\omega}$. Wir bilden nun mit zunächst unbestimmten ganzzahligen Exponenten c_λ den Charakter

$$(3) \qquad \chi(x) = \prod_\lambda \chi_\lambda(x)^{c_\lambda}.$$

Dieser erzeugt eine zyklische Klasseneinteilung modulo $m = K.G.V.[p_1, p_2, \ldots, p_r]$, wobei zwei Zahlen zur gleichen Klasse gerechnet werden, wenn $\chi(x)$ für sie den gleichen Wert hat. Die Klassenzahl ist eine Potenz von l. Wir wollen nun die c_λ so bestimmen, daß keine der Potenzen $a_\varkappa^{l^\nu} (\varkappa = 1, 2, \ldots, r)$ bei dieser Klasseneinteilung in die Einsklasse hineinfällt, d. h. daß

$$(4) \qquad \chi(a_\varkappa)^{l^\nu} \neq 1 \qquad [\varkappa = 1, 2, \ldots, r],$$

oder, wenn man für χ den Wert aus (3) einsetzt,

$$(5) \qquad \prod_\lambda \chi_\lambda(a_\varkappa)^{c_\lambda l^\nu} \neq 1 \qquad [\varkappa = 1, 2, \ldots, r]$$

ist.

---

[5]) Vgl. Sylvester, On the divisors of the sum of a geometrical series, Nature **37** (1888), p. 417; Collected papers IV, p. 625.

Zu dem Zweck bestimmen wir zunächst die Anzahl der Systeme von Restklassen $c_1, \ldots, c_r$ wo c_λ eine Restklasse mod l^{μ_λ} repräsentiert, welche eine der Bedingungen (5), z. B. die erste, *verletzen*, für welche also im Gegenteil

$$\chi_1(a_1)^{c_1 l^\nu} = \chi_2(a_1)^{-c_2 l^\nu} \cdots \chi_r(a_r)^{-c_r l^\nu} \tag{6}$$

ist. Ist in (6) die rechte Seite von höherer Ordnung als die Ordnung l^ω von $\chi_1(a_1)^{l^\nu}$, so gibt es kein c_1, welches (6) erfüllt; sonst gibt es genau ein c_1 mod l^ω, also genau $l^{\mu_1-\omega}$ Restklassen c_1 mod l^{μ_1}, die (6) erfüllen. Somit gibt es höchstens

$$l^{\mu_1-\omega+\mu_2+\cdots+\mu_r} = l^{\Sigma\mu-\omega}$$

Systeme $\{c_1, \ldots, c_r\}$, welche (6) erfüllen, also die erste der Bedingungen (5) verletzen. Dasselbe gilt für alle r Bedingungen (5); mithin gibt es insgesamt höchstens

$$r \cdot l^{\Sigma\mu-\omega} < l^{\Sigma\mu}$$

Systeme $\{c_1, \ldots, c_r\}$, welche (5) verletzen. Es gibt aber $l^{\Sigma\mu}$ Systeme von Restklassen $\{c_1, \ldots, c_r\}$. Unter diesen kommen somit auch solche vor, die (5) erfüllen. Aus (4) folgt dann, daß der Exponent von $\chi(a_\varkappa)$, also der Exponent von $a_\varkappa$ bei unserer Klasseneinteilung, eine höhere Potenz von l ist als l^ν. Damit ist Satz 2 bewiesen.

Zusatz zu Satz 2. Für $l = 2$ kann man die Kongruenzklasseneinteilung außerdem so einrichten, daß -1 zum Exponenten 2 gehört.

Beweis. Gesetzt, in der oben bestimmten, durch $\chi(x)$ vermittelten Klasseneinteilung gehöre -1 zum Exponenten 1, d. h. es sei $\chi(-1) = 1$. Dann wählen wir eine in $a_1 a_2 \cdots a_r$ nicht aufgehende Primzahl p der Form $4m - 1$. Das ist immer möglich, da die Primfaktoren von $4 a_1 a_2 \cdots a_r - 1$ nicht alle von der Form $4m + 1$ sein können. Wir ersetzen nun $\chi(x)$ durch den Charakter

$$\chi'(x) = \chi(x) \cdot \left(\frac{x}{p}\right).$$

Dann ist

$$\chi'(-1) = \left(\frac{-1}{p}\right) = -1,$$

dagegen nach wie vor (wegen $\nu > 0$)

$$\chi'(a_\varkappa)^{2^\nu} = \chi(a_\varkappa)^{2^\nu} \neq 1.$$

Satz 3. *Es gibt bei gegebenen $a_1, \ldots, a_r$ und k eine zyklische Kongruenzklasseneinteilung der rationalen Zahlen, bei der die Exponenten von $a_1, \ldots, a_r$ durch k teilbar sind und -1 den Exponenten 2 hat.*

Beweis. Man kann $k = \Pi l^\nu$ ohne Einschränkung als gerade annehmen. Für jedes einzelne l gibt es nach Satz 2 und dem Zusatz eine zyklische Kongruenzklasseneinteilung mit Klassenzahl l^σ, in der die Exponenten von $a_1, \ldots, a_r$ durch $l^{\nu+1}$ teilbar sind und (für $l = 2$) -1 den Exponenten 2 hat. Die Durchkreuzung (Durchschnittsbildung) aller dieser Klasseneinteilungen ergibt eine Klasseneinteilung mit Klassenzahl Πl^σ, welche zyklisch ist, weil der Durchschnitt der erzeugenden Klassen (mit Exponenten l^σ) eine Klasse vom Exponenten Πl^σ ist. Die Exponenten von $a_1, \ldots, a_r$ in dieser Klasseneinteilung sind durch sämtliche l^ν, also durch k teilbar, und der Exponent von -1 ist 2.

Eingegangen 14. November 1933.

Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper.

Von *Ernst Witt* in Göttingen.

Mit der Darstellung von Funktionen durch Quadrate hat sich zuerst Hilbert beschäftigt. Dann haben Landau und Artin die Untersuchungen darüber fortgeführt.

Hier sollen die Funktionen eines reellen algebraischen Funktionenkörpers k hinsichtlich ihrer Zerlegung in Quadrate untersucht werden, und zwar wird dies unter Verwendung Abelscher Integrale geschehen. Auf diesem Wege wird der letzte Satz der Artinschen Arbeit [1]) für den Fall des Körpers k von neuem bewiesen werden, sogar mit den genaueren Zusätzen:

Ist eine Funktion des Körpers k überhaupt Summe von Quadraten, so ist sie auch schon Summe zweier Quadrate.

Ist -1 überhaupt Summe von Quadraten, dann ist jede Funktion des Körpers k Summe zweier Quadrate.

Sehen wir uns die Verhältnisse genauer an:

Durch die Gleichung $f(x, y) = 0$ mit reellen Koeffizienten sei der reelle algebraische Funktionenkörper k definiert. Seine Elemente α werden wir reelle Funktionen nennen, die Elemente A des Oberkörpers $k(i)$ sollen dagegen komplex heißen. Zum Oberkörper $k(i)$ gehört eine Riemannsche Fläche vom Geschlecht p, diese sei n-blättrig über der x-Kugel. Mit jedem Punkt $\mathfrak{P} = (x, y)$ liegt auch der konjugiert komplexe Punkt $\mathfrak{P}^\sigma = (\overline{x}, \overline{y})$ auf der Fläche. Die Menge der reellen Punkte $\mathfrak{P} = \mathfrak{P}^\sigma$ bilden eine Reihe von geschlossenen Kurven, die sich nicht schneiden. Nach der topologischen Definition des Geschlechtes ist die Anzahl r dieser reellen Kurven eine der Zahlen 0 bis $p + 1$. Auf diesen reellen Kurven sind die Werte jeder Funktion des Körpers k reell oder ∞.

Eine reelle Funktion α werden wir definit nennen, wenn α auf keiner der Kurven das Vorzeichen wechselt, ebenso soll α positiv definit heißen, wenn α auf keiner Kurve negativ wird. Z. B. ist die Zahl -1 immer definit, im nullteiligen Fall ($r = 0$) sogar positiv definit.

Über das Verhalten der reellen Funktionen auf den reellen Kurven werden wir folgendes beweisen:

I. *Ist α positiv definit, so ist $\alpha = \beta^2 + \gamma^2$.*

II. *Wird zu jeder Kurve ein Vorzeichen gewählt, so gibt es definite Funktionen, die genau das verlangte Vorzeichen haben.*

III. *Wird auf jeder Kurve eine gerade Anzahl von verschiedenen Punkten willkürlich markiert, so gibt es Funktionen, die genau an diesen Stellen ihr Vorzeichen wechseln.*

---

[1]) E. Artin, Über die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Hamburg **5** (1927), S. 115.

Zur Einleitung in das zweite Thema dieser Arbeit werden wir einen Satz von Tsen [2]), den dieser unter Verwendung der Eliminationstheorie gewonnen hat, im Fall eines komplexen Funktionskörpers von neuem mit Hilfe der Abelschen Integrale beweisen.

Im zweiten Teil werden wir die Übersetzung des ersten funktionentheoretischen Teiles in die algebraische Sprache vornehmen, und erhalten dadurch eine Übersicht über die sämtlichen Schiefkörper S von endlichem Rang über dem Zentrum k:

I'. *Zerfällt S in jedem $\mathfrak{p}$-adischen Oberkörper $k_\mathfrak{p}$, so zerfällt S schlechthin.*

II'. *Es gibt genau 2^r unverzweigte Schiefkörper.*

III'. *Wird auf jeder Kurve eine gerade Anzahl von Punkten willkürlich markiert, so gibt es gerade 2^r Schiefkörper, die genau an diesen Stellen verzweigt sind. Auf diese Art und Weise findet man alle möglichen Typen von Schiefkörpern.*

Vergleicht man diese Sätze mit der entsprechenden Theorie der Algebren vom Rang 4 über einem algebraischen Zahlkörper k^*, wie sie Hasse [3]) mit Hilfe der Klassenkörpertheorie aufgestellt hat, so fällt einem eine große Analogie auf:

I*. Zerfällt S in jedem $\mathfrak{p}$-adischen Oberkörper $k^*_\mathfrak{p}$, so zerfällt S schlechthin.

II*. Es gibt genau einen unverzweigten Schiefkörper (nämlich den unechten k^* selbst).

III*. Wird eine gerade Anzahl von nichtkomplexen Primstellen willkürlich gewählt, so gibt es gerade einen Schiefkörper, der genau an diesen Stellen verzweigt ist. Auf diese Art und Weise findet man alle möglichen Typen von Schiefkörpern.

Im Gegensatz zu den Schiefkörpern über k^* können also Schiefkörper S über k unverzweigt sein, ferner hat S stets träge Primstellen. Endlich kann es vorkommen, daß es über k überhaupt keine echten Schiefkörper gibt [4]), nämlich genau dann, wenn k nullteilig ($r = 0$) ist.

Was die analytischen Hilfsmittel anbelangt, so spielen offenbar die Abelschen Integrale dieselbe Rolle im Funktionenkörper k wie die ζ-Funktion im Zahlkörper k^*.

1.

Erinnern wir uns zuerst an Bekanntes aus der Theorie der algebraischen Funktionen des Oberkörpers $k(i)$. Das System der Wurzeln $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ und Pole $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m$ einer Funktion A aus $k(i)$ wird als Divisor $\frac{\mathfrak{P}_1, \cdots \mathfrak{P}_m}{\mathfrak{Q}_1 \cdots \mathfrak{Q}_m} = (A)$ geschrieben, allgemein nennt man einen Bruch $\frac{\mathfrak{P}_1 \cdots \mathfrak{P}_m}{\mathfrak{Q}_1 \cdots \mathfrak{Q}_l} = \mathfrak{D}$ aus beliebigen Punkten $\mathfrak{P}_1, \ldots, \mathfrak{Q}_l$ der Riemannschen Fläche einen Divisor der Ordnung $m - l$. Den konjugiert komplexen Divisor $\frac{\mathfrak{P}_1^\sigma \cdots \mathfrak{P}_m^\sigma}{\mathfrak{Q}_1^\sigma \cdots \mathfrak{Q}_l^\sigma}$ bezeichnen wir mit $\mathfrak{D}^\sigma$. Im Fall $\mathfrak{D} = \mathfrak{D}^\sigma$ sagen wir, $\mathfrak{D}$ sei reell. Für reelle Divisoren verwenden wir auch kleine deutsche Buchstaben. Es bedeutet

(1) $\qquad (\alpha) = \mathfrak{A}^{1+\sigma}$ dasselbe wie α ist definit,

(2) $\qquad \alpha = A^{1+\sigma}$ dasselbe wie $\alpha = \beta^2 + \gamma^2$.

---

[2]) Ch. Tsen, Divisionsalgebren über Funktionenkörpern. Gött. Nachr. 1933, S. 335.

[3]) H. Hasse, Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Math. Ann. 107 (1933), S. 731. — Siehe auch E. Witt, Riemann-Rochscher Satz und Z-Funktion im Hyperkomplexen. Math. Ann. 109 (1934).

[4]) Die Frage nach diesen universellen Zerfällungskörpern hat zuerst Ch. Tsen in seiner Dissertation (Göttingen 1933) aufgeworfen. Es sind gerade die Zerfällungskörper der Quaternionen.

Denn $(\alpha) = \mathfrak{A}^{1+\sigma}$ bedeutet: die Wurzeln und Pole von α auf den reellen Kurven sind sämtlich von gerader Ordnung, d. h. aber α wechselt nirgends das Vorzeichen. Bei (2) ist $(\beta + i\gamma)^{1+\sigma} = \beta^2 + \gamma^2$ zu beachten.

du_ν seien p linear unabhängige überall endliche Differentiale aus dem Körper k; wir fassen sie zu einem Vektor du zusammen. Nach Wahl der Integrationswege bezeichnen wir den Vektor

$$\int_{\mathfrak{O}_1}^{\mathfrak{P}_1} du + \cdots + \int_{\mathfrak{O}_m}^{\mathfrak{P}_m} du \quad \text{kurz mit } L\left(\frac{\mathfrak{P}_1 \cdots \mathfrak{P}_m}{\mathfrak{O}_1 \cdots \mathfrak{O}_m}\right).$$

In dieser Schreibweise gilt

$$(3) \qquad \begin{cases} L(\mathfrak{A}\mathfrak{B}) = L(\mathfrak{A}) + L(\mathfrak{B}) \\ L(\mathfrak{A}^{-1}) = -L(\mathfrak{A}) \\ L(\mathfrak{A}^{\sigma}) = \overline{L(\mathfrak{A})}, \end{cases}$$

das Zeichen L soll also an die Eigenschaften des Logarithmus erinnern.

Das *Abel*sche *Theorem* lautet:

(4) Genau dann ist $\mathfrak{A} = (A)$, wenn $L(\mathfrak{A}) \equiv 0 \pmod{\text{Per.}}$ gilt.

Und das *Jacobi*sche *Theorem*:

(5) $L\left(\frac{\mathfrak{X}_1 \cdots \mathfrak{X}_p}{\mathfrak{O}^p}\right)$ durchläuft bei festem Punkt $\mathfrak{O}$ und variablen Punkten $\mathfrak{X}_1, \ldots, \mathfrak{X}_p$ alle Vektoren.

Hurwitz [5]) hat auf algebraischem Wege für die Perioden reeller Abelscher Integrale eine Basis von folgender Gestalt gefunden:

$$(6) \qquad \begin{array}{l} R_1, \ldots, R_q, \quad R_{q+1} \qquad\quad , \ldots, \quad R_p \qquad , \\ I_1, \ldots, I_q, \frac{1}{2}R_{q+1} + I_{q+1}, \ldots, \frac{1}{2}R_p + I_p; \end{array}$$

dabei sind R_ν reelle und I_ν imaginäre Vektoren. Bezeichnen wir wieder mit r die Anzahl der reellen Kurven auf der Riemannschen Fläche, so ist nach Weichold [6])

$$(7) \qquad q = \begin{cases} r-1 & \text{falls } r \neq 0 \\ 0 & \text{falls } r = 0,\ p \text{ gerade} \\ 1 & \text{falls } r = 0,\ p \text{ ungerade}. \end{cases}$$

2.

Nach Festlegung der Bezeichnung und Angabe der bisher bekannten Tatsachen können wir nun daran gehen, unsere funktionentheoretischen Sätze zu beweisen.

Satz 1. Ist x positiv definit, so ist $(x) = (A)^{1+\sigma}$.

Beweis. Nach Definition des Positiv-Definiten liegt keine reelle Kurve der Riemannschen Fläche über der negativen x-Achse. Die n Wege, die über der negativen x-Achse liegen, lassen sich daher in Paare konjugiert komplexer Wege einteilen: $w_1, w_1^\sigma, \ldots, w_{\frac{n}{2}}, w_{\frac{n}{2}}^\sigma$. Wir bilden jetzt einen Divisor $\mathfrak{A}$, indem wir die über $x = 0$ gelegenen Punkte von $w_1, \ldots, w_{\frac{n}{2}}$ in den Zähler, und die über $x = \infty$ gelegenen in den Nenner schreiben. Dann besteht aber der Divisor $\mathfrak{A}^{1+\sigma}$ gerade aus den Wurzeln und

[5]) Hurwitz, Über eindeutige $2n$-fach periodische Funktionen. Math. Werke I, S. 99.

[6]) Weichold, Über symmetrische Riemannsche Flächen usw. Ztschr. f. Math. u. Phys. 28 (1883), S. 321. — F. Klein, Realitätsverhältnisse bei den Normalkurven der φ, Ges. Abh. II, S. 170. — Auf diese Literatur machte mich Herglotz aufmerksam. Übrigens hat zuerst Herglotz bestätigt, daß im elliptischen nullteiligen Körper jede Funktion Summe von zwei Quadraten ist.

Polen der Funktion x auf der Riemannschen Fläche, d. h. $\mathfrak{A}^{1+\sigma} = (x)$. Nun ist $L(x) = 0$, wenn über die vorgelegten Wege integriert wird [7]). Dies bedeutet: $L(\mathfrak{A})$ ist imaginär. Lösen wir nach dem Jacobischen Theorem (5) die Gleichung $L(\mathfrak{X}) = -\frac{1}{2} L(\mathfrak{A})$ auf, so ist $L(\mathfrak{A}\mathfrak{X}^{1-\sigma}) = 0$, also ist nach dem Abelschen Theorem (4) $\mathfrak{A}\mathfrak{X}^{1-\sigma} = (A)$, daraus folgt aber $(x) = (A)^{1+\sigma}$.

Satz 2. Ist $r = 0$, so ist $-1 = A^{1+\sigma}$.

Wir bemerken zuerst: Ist $A^{1+\sigma} = a > 0$, so hat (A) die Form $(B)^{1-\sigma}$. Denn für konstantes A ist $(A) = (1)^{1-\sigma}$. Anderenfalls ist $(A) = (A + \sqrt{a})^{1-\sigma}$.

Es ist weiter zu beachten, daß infolge $r = 0$ jeder reelle Divisor $\mathfrak{d}$ die Form $\mathfrak{D}^{1+\sigma}$ hat, also von gerader Ordnung ist.

Nun zum Beweis des Satzes. Es sei $\mathfrak{O}$ ein fester Punkt auf der Riemannschen Fläche, wir setzen $L(\mathfrak{O}^{1-\sigma}) = U + iV$. Addieren wir diese Gleichung zu ihrer konjugiert komplexen, so erhalten wir die Tatsache, daß U eine halbe reelle Periode ist. Jetzt müssen wir zwei Fälle unterscheiden.

Erstens sei $q = 0$, dann ersehen wir aus (6), daß U (mod. Per.) einem imaginären Vektor kongruent ist. D. h. durch passende Verlegung des Integrationsweges wird $L(\mathfrak{O}^{1-\sigma})$ imaginär. Nach dem Jacobischen Theorem können wir einen Divisor $\mathfrak{x} = \mathfrak{x}_1 \cdots \mathfrak{x}_{2p+1}$ so wählen, daß

$$L\left(\frac{\mathfrak{x}}{\mathfrak{O}^{2p+1}}\right) = -\frac{2p+1}{2} L(\mathfrak{O}^{1-\sigma}),$$

also imaginär wird. Es folgt daraus

$$L(\mathfrak{x}^{1-\sigma}) = L\left(\frac{\mathfrak{x}}{\mathfrak{O}^{2p+1}}\right) + L\left(\frac{\mathfrak{O}^{(2p+1)\sigma}}{\mathfrak{x}^{\sigma}}\right) + (2p+1)\, L(\mathfrak{O}^{1-\sigma}) = 0.$$

Nach dem Abelschen Theorem bedeutet das $\mathfrak{x}^{1-\sigma} = (A)$, also ist $A^{1+\sigma}$ konstant. Wäre $\mathfrak{x}^{1-\sigma} = (B)^{1-\sigma}$, so auch $\mathfrak{x} = \mathfrak{d}(B)$, was mit den Ordnungen nicht stimmt. Aus $(A) \neq (B)^{1-\sigma}$ folgt aber nach der gemachten Bemerkung $A^{1+\sigma} < 0$.

Zweitens sei $q \neq 0$. Nach dem Jacobischen Theorem können wir einen Divisor $\mathfrak{x} = \mathfrak{x}_1 \cdots \mathfrak{x}_{2p}$ so wählen, daß

$$L\left(\frac{\mathfrak{x}}{\mathfrak{O}^{2p}}\right) = \tfrac{1}{2} I - piV$$

wird, wobei I die erste imaginäre Periode in der Basis (6) sein möge. Es folgt daraus

$$L(\mathfrak{x}^{1-\sigma}) = L\left(\frac{\mathfrak{x}}{\mathfrak{O}^{2p}}\right) + L\left(\frac{\mathfrak{O}^{2p\sigma}}{\mathfrak{x}^{\sigma}}\right) + 2pL(\mathfrak{O}^{1-\sigma}) \equiv 0,$$

nach dem Abelschen Theorem bedeutet das $\mathfrak{x}^{1-\sigma} = (A)$, also ist $A^{1+\sigma}$ konstant. Wäre $\mathfrak{x}^{1-\sigma} = (B)^{1-\sigma}$, so auch $\mathfrak{x} = \mathfrak{D}^{1+\sigma}$ (B), oder nach dem Abelschen Theorem

$$\tfrac{1}{2} I - piV = L\left(\frac{\mathfrak{x}}{\mathfrak{O}^{2p}}\right) \equiv L\left(\frac{\mathfrak{D}}{\mathfrak{O}^{p}}\right) + \overline{L\left(\frac{\mathfrak{D}}{\mathfrak{O}^{p}}\right)} + p\,\overline{L(\mathfrak{O}^{1-\sigma})},$$

d. h. $\frac{1}{2} I$ wäre einem reellen Vektor kongruent, was sich nicht mit der Gestalt der Basis (6) verträgt. Aus $(A) \neq (B)^{1-\sigma}$ folgt jetzt wieder $A^{1+\sigma} < 0$. Damit ist Satz 2 vollständig bewiesen.

Nun sind wir so weit, daß wir unsere erste Behauptung beweisen können.

---

[7]) H. Weyl, Die Idee der Riemannschen Fläche, S. 136.

I. *Ist α positiv definit, so ist $\alpha = \beta^2 + \gamma^2$.*

Für konstantes α ist nämlich I im wesentlichen identisch mit Satz 2.

Für variables α ist $(\alpha) = (A)^{1+\sigma}$, da das Element x aus Satz 1 im Körper k nicht ausgezeichnet ist. Für $r = 0$ sind darin nach Satz 2 die Klammern unwesentlich. Und für $r \neq 0$ muß eine der beiden Gleichungen

$$A^{1+\sigma} = \alpha, \quad A^{1+\sigma} = -\alpha$$

bis auf einen positiven Faktor richtig sein. Da nun $A^{1+\sigma}$ positiv definit ist, $-\alpha$ aber nicht, kann es nur die erste Gleichung sein; das ist gerade die Behauptung I.

3.

Im Fall $r = 0$ sind II und III leere Aussagen, so daß wir in diesem Abschnitt $r \neq 0$ annehmen dürfen.

Bezeichnen wir mit $\mathfrak{A}_1$ diejenigen Divisoren, deren Norm $\mathfrak{A}_1^{1+\sigma} = (A)$ ist, so gilt der

Satz 3. Die Gruppe der Divisoren von der Form $\mathfrak{D}^{1-\sigma}(A)$ hat in der Gruppe $\mathfrak{A}_1$ den Index 2^q.

Beweis. Nach dem Abelschen Theorem brauchen wir nur den Index der additiven Gruppe $L(\mathfrak{D}^{1-\sigma})$ in der Gruppe $L(\mathfrak{A}_1)$ (mod. Per.) festzustellen. $\mathfrak{o}$ sei ein reeller Punkt. Ist $\mathfrak{D}$ ein Divisor der Ordnung d, so ist $L(\mathfrak{D}^{1-\sigma}) = L\left(\frac{\mathfrak{D}}{\mathfrak{o}^d}\right) - \overline{L\left(\frac{\mathfrak{D}}{\mathfrak{o}^d}\right)}$ ein imaginärer Vektor. Umgekehrt, ist iU ein imaginärer Vektor, so gibt es nach dem Jacobischen Theorem einen Vektor $\mathfrak{D} = \mathfrak{x}_1 \ldots \mathfrak{x}_p$ mit $L\left(\frac{\mathfrak{D}}{\mathfrak{o}^p}\right) = \frac{i}{2}U$, woraus $L(\mathfrak{D}^{1-\sigma}) = iU$ folgt. $L(\mathfrak{D}^{1-\sigma})$ durchläuft also (mod. Per.) genau alle imaginären Vektoren. Anderseits durchläuft offenbar $L(\mathfrak{A}_1)$ genau die Vektoren von der Form $\frac{1}{2}R + iV$, wobei R die reellen Perioden und iV alle imaginären Vektoren durchläuft. Aus der Gestalt der Basis (6) folgt nun, daß der Index gerade 2^q ist.

In der Gleichung $\mathfrak{A}_1^{1+\sigma} = (A)$ ist $A^{1-\sigma}$ eine Konstante a mit $a^{1+\sigma} = 1$. Ist A noch keine reelle Funktion, d. h. $a \neq 1$, so können wir A durch die nunmehr reelle Funktion $\alpha_1 = \frac{iA}{1-a}$ ersetzen, so daß immer $\mathfrak{A}_1^{1+\sigma} = (\alpha_1)$ gilt.

In (1) haben wir schon bemerkt, daß diejenigen Funktionen α_1 mit der Eigenschaft $(\alpha_1) = \mathfrak{A}_1^{1+\sigma}$ gerade die Gruppe der definiten Funktionen ausmachen. Nach I können wir nun die Behauptung II in der gleichwertigen Form aussprechen:

II. *Der Index $(\alpha_1 : A^{1+\sigma})$ hat den Wert 2^r.*

Beweis. Beim Übergang zu Divisoren ergibt sich $(\alpha_1 : A^{1+\sigma}) = 2 \cdot (\mathfrak{A}_1^{1+\sigma} : (A)^{1+\sigma})$. Wird die leicht einzusehende Tatsache beachtet, daß die Divisoren $\mathfrak{A}$ mit der Eigenschaft $\mathfrak{A}^{1+\sigma} = (1)$ immer die Form $\mathfrak{D}^{1-\sigma}$ haben, so folgt beim Übergang zu den Normen $2^q = (\mathfrak{A}_1 : \mathfrak{D}^{1-\sigma}(A)) = (\mathfrak{A}_1^{1+\sigma} : (A)^{1+\sigma})$; also gilt $(\alpha_1 : A^{1+\sigma}) = 2^{q+1}$. Damit sind wir fertig, wenn wir noch das Resultat (7) von Weichold beachten.

Weisen wir jetzt die letzte Behauptung nach.

III. *Wird auf jeder Kurve eine gerade Anzahl von verschiedenen Punkten willkürlich markiert, so gibt es Funktionen, die genau an diesen Stellen ihr Vorzeichen wechseln.*

Wir bilden einen Divisor $\mathfrak{a}$, der aus den markierten Punkten besteht, und zwar sollen die Punkte jeder Kurve zur Hälfte im Zähler, zur anderen Hälfte im Nenner stehen.

Die zu $\mathfrak{a}$ gehörigen Wege mögen auf den Kurven selbst liegen, so daß $L(\mathfrak{a})$ reell ist. Nach dem Jacobischen Theorem lösen wir $L(\mathfrak{X}) = -\frac{1}{2} L(\mathfrak{a})$, dann folgt $L(\mathfrak{a}\mathfrak{X}^{1+\sigma}) = 0$, also nach dem Abelschen Theorem $\mathfrak{a}\mathfrak{X}^{1+\sigma} = (A)$. Ersetzen wir darin ebenso wie vorhin A durch eine reelle Funktion α, so hat α genau die verlangten Vorzeichenwechsel.

4.

In diesem Abschnitt soll k ein komplexer Funktionenkörper sein, K bedeute eine endliche Erweiterung von k. Wir wollen jetzt den neuen Beweis des Satzes von Tsen bringen.

Satz 4. Jedes Element x aus k ist Norm eines Elementes A aus K.

Wir können gleich annehmen, x sei variabel. Bezeichnet Ω den Körper aller komplexen Zahlen, so sei $k = \Omega(x, y)$. G sei ein Galoisscher Oberkörper von $K/\Omega(x)$. Die zu den Körpern $\Omega(x), k, K, G$ gehörigen Gruppen seien $\mathfrak{G}$, $\mathfrak{g}$, $\mathfrak{h}$, 1. Diese Buchstaben sollen gleichzeitig die Summen der Gruppenelemente bedeuten, so daß wir die Zerlegung nach Nebengruppen in der Form $\mathfrak{G} = \mathfrak{g}(G_1 + G_2 + \cdots)$ und $\mathfrak{g} = (g_1 + g_2 + \cdots)\,\mathfrak{h}$ schreiben können.

Die Riemannsche Fläche des Körpers G denken wir uns über der x-Kugel ausgebreitet. Wir gehen jetzt ebenso vor wie beim Beweis des Satzes 1. Wir greifen unter den Wegen über der negativen x-Achse einen Weg mit den Endpunkten $\mathfrak{P}$ und $\mathfrak{Q}$ heraus. Dann ist $\left(\frac{\mathfrak{P}}{\mathfrak{Q}}\right)^{\mathfrak{G}} = (x)$, infolgedessen ist $\mathfrak{G} \cdot L\left(\frac{\mathfrak{P}}{\mathfrak{Q}}\right) = 0$. Bezeichnen wir mit $\mathfrak{A}$ den Divisor $\left(\frac{\mathfrak{P}}{\mathfrak{Q}}\right)^{G_1+G_2+\cdots}$, so ist $\mathfrak{g} L(\mathfrak{A}) = 0$. $\mathfrak{g}$ bestehe aus g Elementen. Lösen wir nach dem Jacobischen Theorem die Gleichung $L(\mathfrak{X}) = \frac{1}{g} L(\mathfrak{A})$, und setzen noch $\mathfrak{B} = \mathfrak{X}^{g-\mathfrak{g}}$, so folgt aus dem Bisherigen $L(\mathfrak{B}) = (g - \mathfrak{g})\frac{1}{g} L(\mathfrak{A}) = L(\mathfrak{A})$. Nach dem Abelschen Theorem bedeutet dies $\mathfrak{A} = (A)\mathfrak{B}$. Unter Beachtung von $\mathfrak{A}^{\mathfrak{g}} = (x)$ und $\mathfrak{B}^{\mathfrak{g}} = (1)$ folgt daraus $(x) = (A)^{\mathfrak{g}} = (A^{\mathfrak{h}})^{g_1+g_2\cdots}$, somit ist x bis auf eine unwesentliche Konstante die Norm des Elementes $A^{\mathfrak{h}}$ aus dem Körper K.

Es ist leicht zu sehen, daß Satz 4 auch noch richtig bleibt, wenn für k ein reeller nullteiliger Funktionenkörper genommen wird: Wir betrachten die Körper k, $k(i)$, K, $K(i)$. Jedes Element α aus k ist nach I Norm eines Elementes α_i aus $k(i)$. Nach Satz 4 ist α_i Norm eines Elementes A_i aus $K(i)$. Ist A die Norm von A_i, von $K(i)$ nach K genommen, so ist α aus k Norm des Elementes A aus K.

Mit seinem Satz hat Tsen[2]) unter Verwendung Sylowscher Sätze bewiesen, daß es über einem komplexen Funktionenkörper keine echten Schiefkörper gibt. (Einen direkteren Beweis für diese Tatsache hat Artin[4]) angegeben.) Jedenfalls läßt sich schon jetzt sagen, daß es auch über reellen nullteiligen Funktionenkörpern keine Schiefkörper endlichen Ranges gibt.

5.

Wir müssen nun noch unsere bisherigen Resultate in das Algebraische übertragen. Der Übersicht halber werden wir hier nicht ins Einzelne gehen, da die dazu notwendigen Schlußweisen schon hinreichend bekannt sind, sondern wir wollen nur das Wichtigste

[3]) H. Hasse, Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. Math. Ann. 104 (1931) S. 495.

hervorheben. Bezüglich der allgemeinen Theorie verweisen wir auf die Darstellung bei Hasse [3] [8]).

Mit (α, β) bezeichnen wir das einfache System, daß aus den Basisgrößen $1, u, v, uv$ besteht und für das die Rechenregeln $u^2 = \alpha$, $v^2 = \beta$, $uv = -vu$ gelten.

Jeder Schiefkörper S über einem reellen algebraischen Funktionenkörper k läßt sich in der Gestalt $(\alpha, -1)$ schreiben, da $k(i)$ Zerfällungskörper von jedem Schiefkörper S ist.

$(\alpha, -1) \sim 1$ ist gleichwertig mit $\alpha = \beta^2 + \gamma^2$, oder nach I mit der Aussage, α ist positiv definit.

$(\alpha, -1) \sim (\beta, -1)$ ist gleichwertig mit der Aussage, α und β haben auf allen reellen Kurven dasselbe Vorzeichen.

Studieren wir jetzt das Verhalten von $(\alpha, -1)$ an der lokalen Stelle $\mathfrak{p}$. Ist $\mathfrak{p} = \mathfrak{P}^{1+\sigma}$, so ist der Restklassenkörper mod $\mathfrak{p}$ algebraisch abgeschlossen, deshalb zerfällt $(\alpha, -1)_\mathfrak{p}$. Ist dagegen $\mathfrak{p} = \mathfrak{P}$, so führen wir die Bezeichnungen $\alpha(\mathfrak{p}) > 0$, $\alpha(\mathfrak{p}) < 0$, $\alpha(\mathfrak{p}) \gtrless 0$ ein für das entsprechende Verhalten von α auf der reellen Kurve in der Umgebung des Punktes $\mathfrak{P}$. Beim Zeichen $>$ oder $<$ geht $\mathfrak{p}$ in gerader Ordnung in α auf, dagegen beim Zeichen $\gtrless$ in ungerader Ordnung. Wird dies beachtet, so folgt leicht nach der allgemeinen Theorie:

Ist $\alpha(\mathfrak{p}) > 0$, so zerfällt $(\alpha, -1)_\mathfrak{p}$.

Ist $\alpha(\mathfrak{p}) < 0$, so ist $(\alpha, -1)_\mathfrak{p} \simeq (-1, -1)_\mathfrak{p}$ und zerfällt nicht. $\mathfrak{p}$ ist träge in $(\alpha, -1)$.

Ist $\alpha(\mathfrak{p}) \gtrless 0$, so zerfällt $(\alpha, -1)_\mathfrak{p}$ nicht. Aus $\alpha = u^2$ folgt, $\mathfrak{p}$ ist verzweigt in $(\alpha, -1)$. Die $\mathfrak{p}$-Diskriminante und $\mathfrak{p}$-Differente von $(\alpha, -1)$ lautet $\mathfrak{p}^2$ bzw. $\mathfrak{p}^1$.

In diesen Ausführungen sind die Behauptungen I', II', III' enthalten.

Satz 5. Durch $\alpha(\mathfrak{p}) < 0$, $\beta(\mathfrak{p}) < 0$ sind fast alle (d. h. bis auf endlich viele) Primstellen gegeben, die sich in (α, β) träge verhalten.

Beweis. $1, u, v, uv$ ist für fast alle $\mathfrak{p}$ die Basis einer Maximalordnung, wir brauchen nämlich nur diejenigen endlich vielen $\mathfrak{p}$ auszuschließen, die in der Basisdiskriminante $-16\alpha^2\beta^2$ oder in der Multiplikationstafel vorkommen. Das Restklassensystem (α, β) mod $\mathfrak{p}$ ist genau dann ein Schiefkörper, wenn zugleich $\alpha(\mathfrak{p})$ und $\beta(\mathfrak{p}) < 0$ ist.

Aus der Tatsache, daß durch Angabe fast aller trägen Primstellen ein Schiefkörper vollkommen festgelegt ist, ergibt sich somit aus Satz 5 ein genaues Kriterium für die Isomorphie zwischen (α, β) und (α', β').

$k(\vartheta)$ sei endliche Erweiterung von k. ϑ sei Wurzel des irreduziblen normierten Polynoms $F(t)$. Für diejenigen $\mathfrak{p} = \mathfrak{P}$, die nicht zufällig Pole der Koeffizienten von $F(t)$ sind, führen wir das Polynom $F_\mathfrak{p}(t)$ ein, das aus $F(t)$ entsteht, indem jeder Koeffizient durch seinen reellen Wert an der Stelle $\mathfrak{p}$ ersetzt wird. Mit dieser Festsetzung gilt der

Satz 6. $k(\vartheta)$ ist genau dann Zerfällungskörper von S, wenn $F_\mathfrak{p}(t)$ für fast keine trägen $\mathfrak{p}$ reelle Wurzeln hat.

6.

Zum Schluß wollen wir einige weniger tiefschürfende Betrachtungen anstellen.

Reelle Funktionenkörper vom Geschlecht Null gibt es bis auf birationale Transformationen nur zwei, nämlich $\mathsf{P}(x)$ und $\mathsf{P}(x, \sqrt{-1 - x^2})$. Dieser zweite nullteilige Körper ist abstrakt in jedem reellen nullteiligen Körper k enthalten. Denn nach Satz 2 ist $-1 = \xi^2 + \eta^2$ in k, darin müssen ξ, η variabel sein, und k enthält den Körper $\mathsf{P}(\xi, \sqrt{-1 - \xi^2})$. In einem nicht-nullteiligen Körper kann natürlich $\mathsf{P}(x, \sqrt{-1 - x^2})$ nicht abstrakt vorkommen, sonst wäre -1 Summe zweier Quadrate.

Wir haben gesehen, daß in einem reellen nullteiligen Körper jedes Element Summe zweier Quadrate ist, obwohl die Zahl i darin nicht vorkommt. Auch der Körper aus 3 Elementen hat diese Eigenschaft. Dagegen ist in einem algebraischen Zahlkörper k ein ähnliches Verhalten unmöglich: Wir wählen zwei Primideale, die sich in $k(i)$ träge verhalten. Wie schon in III* erwähnt wurde, ist dadurch ein Schiefkörper S festgelegt, und zwar zerfällt dieser in $k(i)$. Deshalb hat S die Gestalt $(\alpha, -1)$, und α wäre doch nicht Summe zweier Quadrate. Auch in einem $\mathfrak{p}$-adischen Zahlkörper ist ein ähnliches Verhalten unmöglich, was man sofort mit Hilfe des Schiefkörpers vom Range 4 einsieht.

Als Letztes bringen wir folgenden

Satz 7. k sei ein abstrakter Körper mit Char. $\neq 2$. Jedes Element von k sei Summe zweier Quadrate. Dann hat auch jeder quadratische Oberkörper K diese Eigenschaft. (Also auch jeder Galoissche Oberkörper vom Grade 2^r).

Beweis. Sei $\theta^2 + p\theta + q = 0$ $(q \neq 0)$. Dann soll θ durch zwei Quadrate in $k(\theta)$ dargestellt werden, oder die Gleichung

$$r\theta = (a + c\theta)^2 + (b + d\theta)^2 \qquad (r \neq 0)$$

muß eine Lösung haben. Dies umgeformt gibt

$$a^2 + b^2 = (c^2 + d^2)q, \quad 2(ac + bd) \neq (c^2 + d^2)p.$$

Ist $q = x^2 + y^2$ $(x \neq 0)$, so ist mit passendem Vorzeichen $a, b, c, d = \pm x, y, 1, 0$ eine Lösung.

Göttingen, Sylvester 1933.

Eingegangen 1. Januar 1934.

Zur Theorie der Geschlechtermoduln.

Von *S. Iyanaga* in Paris.

Die Theorie der Führer relativ-abelscher Zahlkörper ist neulich von Hasse auf sehr übersichtliche Weise begründet worden [1]). Es sei mir gestattet, die schon einmal von Herbrand und mir behandelte Theorie der „Geschlechtermoduln" hier erneut darzustellen [2]), nämlich diese Theorie in besseren Anschluß an die Hassesche Führertheorie zu bringen. Einige kleine Unvollkommenheiten, die sich in der früheren Literatur finden, sollen dabei behoben werden [3]).

§ 1. Vorbereitendes.

Zunächst legen wir die Bezeichnungen fest und führen zugleich die Sätze an, auf denen unsere späteren Beweise beruhen.

1. Es sei k ein algebraischer Zahlkörper endlichen Grades; K eine endliche galoissche Erweiterung von k; $\mathfrak{p}$ ein festes Primideal in k; $\mathfrak{P}, \mathfrak{P}', \ldots$ die Primteiler von $\mathfrak{p}$ in K. Unter „Verzweigungskörperreihe" zu $\mathfrak{P}$ für K/k verstehen wir die Reihe der Hilbertschen Körper:

$$k \leqq K_0 < K_1 < \cdots < K_r = K,$$

wobei K_0 der Trägheitskörper, oder, wie wir auch sagen wollen, der „0-te Verzweigungskörper" zu $\mathfrak{P}$ für K/k ist, und weiterhin nur die *verschiedenen* unter den Hilbertschen Verzweigungskörpern aufgezählt sind. K_i soll bei der vollen Zählung der $(v_i + 1)$-te, . . ., v_{i+1}-te Verzweigungskörper sein. Ferner bedeute n_i den Grad von K über K_i (d. i. die Ordnung der entsprechenden Verzweigungsgruppe). Die Zahlen

$$-1 = v_0 < v_1 < \cdots < v_r = v, \qquad (v_{r+1} = \infty),$$
$$n_0 > n_1 > \cdots > n_r = 1$$

sind von Hasse als „charakteristische Invarianten" zu $\mathfrak{P}$ für K/k bezeichnet. Die v_i heißen auch „Verzweigungszahlen".

2. Nun sei Ω ein Teilkörper von K/k : $k \leqq \Omega \leqq K$.

$$\Omega \leqq \bar{K}_0 < \bar{K}_1 < \cdots < \bar{K}_{\bar{r}} = K,$$
$$-1 = \bar{v}_0 < \bar{v}_1 < \cdots < \bar{v}_{\bar{r}} = \bar{v},$$
$$\bar{n}_0 > \bar{n}_1 > \cdots > \bar{n}_{\bar{r}} = 1$$

---

[1]) H. Hasse: Normenresttheorie galoisscher Zahlkörper mit Anwendung auf Führer und Diskriminante abelscher Zahlkörper, erscheint demnächst in Journ. Coll. Science. Tokyo (zit. mit HN). Eine vorläufige Mitteilung ist in zwei Noten in den Comptes Rendus Paris 1933 erschienen. Herr Prof. Hasse hat mir freundlicherweise den Inhalt dieser Arbeit brieflich mitgeteilt und das Manuskript noch vor der Veröffentlichung zur Verfügung gestellt. Ferner hat er mir die Beweismethode für die Herbrandsche Formel, wie sie in § 2 durchgeführt werden wird, angedeutet und mir so die Anregung zur Publikation dieser Note gegeben. Für alles das möchte ich ihm auch hier meinen besten Dank ausdrücken.

[2]) J. Herbrand: Sur la théorie du genre principal, Abh. Hamb. Sem. **9** (1932) (zit. mit HG). S. Iyanaga: Über den allgemeinen Hauptidealsatz, Jap. Journ. of Math. (1930) (zit. mit IH). Das Kenntnis dieser Arbeiten wird nicht vorausgesetzt; alle dortigen Resultate werden neu hergeleitet.

[3]) Vgl. die späteren Anm. [7]), [9]).

mögen die Verzweigungskörperreihe bzw. die charakteristischen Invarianten zu $\mathfrak{P}$ für K/Ω darstellen. Die Körper $\bar{K}_i$ bestimmen sich aus K_i und Ω bekanntlich so:

$$\begin{aligned}\bar{K}_0 &= \Omega K_{\sigma_0} = \Omega K_{\sigma_0+1} = \cdots = \Omega K_{\sigma_1-1} < \bar{K}_1 \\ &= \Omega K_{\sigma_1} = \cdots = \Omega K_{\sigma_2-1} < \cdots < \bar{K}_{\bar{r}} = \Omega K_{\sigma_{\bar{r}}} = \Omega K_\sigma = K.\end{aligned}$$

Dabei ist gesetzt: $\sigma_0 = 0$, $\sigma_{\bar{r}} = \sigma$. σ ist also die Nummer des kleinsten K_i, so daß $\Omega K_i = K$ wird. Die zugehörigen Verzweigungszahlen sind gegeben durch:

(1) $$\bar{v}_0 = v_{\sigma_0} (= v_0 = -1), \quad \bar{v}_1 = v_{\sigma_1}, \ldots, \bar{v}_{\bar{r}} = v_{\sigma_{\bar{r}}} = v_\sigma.$$

Bezeichnet man mit n'_i den Grad von K über ΩK_i, so gilt ferner:

(2) $$\bar{n}_0 = n'_{\sigma_0} = \cdots = n'_{\sigma_1-1}, \quad \bar{n}_1 = n'_{\sigma_1} = \cdots = n'_{\sigma_2-1}, \ldots, \bar{n}_{\bar{r}} = n'_\sigma = 1.$$

3. Wir nehmen jetzt weiterhin an, Ω/k sei galoissch. $\bar{\mathfrak{p}}, \bar{\mathfrak{p}}', \ldots$ seien die verschiedenen Primteiler von $\mathfrak{p}$ in Ω; $\mathfrak{P} \mid \bar{\mathfrak{p}}$. Die Verzweigungskörperreihe bzw. die charakteristischen Invarianten zu $\bar{\mathfrak{p}}$ für Ω/k bezeichnen wir so:

$$\begin{aligned}k \leqq \Omega_0 < \Omega_1 < \cdots < \Omega_\varrho &= \Omega, \\ -1 = \varphi_0 < \varphi_1 < \cdots < \varphi_\varrho &= \varphi, \\ v_0 > v_1 > \cdots > v_\varrho &= 1.\end{aligned}$$

Nun gibt die Herbrandsche Regel [4]) den Zusammenhang zwischen den K_i und Ω_i an. Sie besagt nämlich:

$$\begin{aligned}\Omega_0 = \Omega \cap K_{\tau_0} = \Omega \cap K_{\tau_0+1} = \cdots = \Omega \cap K_{\tau_1-1} < \Omega_1 = \Omega \cap K_{\tau_1} = \cdots = \Omega \cap K_{\tau_2-1} < \cdots < \Omega_\varrho \\ = \Omega \cap K_{\tau_\varrho} = \Omega \cap K_\tau = \Omega,\end{aligned}$$

wobei $\tau_0 = 0$, $\tau_\varrho = \tau$ gesetzt ist. τ ist also die Nummer des kleinsten K_i, der Ω umfaßt. Die Verzweigungszahlen sind durch folgende Formeln bestimmt:

$$\varphi_i - \varphi_0 = \frac{n'_0}{n'_0}(v_1 - v_0) + \frac{n'_1}{n'_0}(v_2 - v_1) + \cdots + \frac{n'_{\tau_i-1}}{n'_0}(v_{\tau_i} - v_{\tau_i-1}), \quad i = 1, 2, \ldots, \varrho;$$

also insbesondere:

(3) $$\varphi - \varphi_0 = \frac{n'_0}{n'_0}(v_1 - v_0) + \frac{n'_1}{n'_0}(v_2 - v_1) + \cdots + \frac{n'_{\tau-1}}{n'_0}(v_\tau - v_{\tau-1}).$$

Ferner gilt offenbar:

(4) $$v_0 n'_0 = n_0 \text{ und allgemein } v_i n'_j = n_j \quad \text{für} \quad \tau_i \leqq j < \tau_{i+1}.$$

4. Wir bemerken, daß die obigen Sätze auch für unendliche Primstellen gültig bleiben, wenn wir folgende Bezeichnungen zugrundelegen:

Eine Primstelle $\mathfrak{P}_\infty$ in K „teilt" eine solche $\mathfrak{p}_\infty$ in k, in Zeichen $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$, wenn die durch $\mathfrak{P}_\infty$ gelieferte Bewertung von K den Zahlen von k dieselben Werte zuordnet wie die $\mathfrak{p}_\infty$ entsprechende Bewertung von k. Wenn $\mathfrak{P}_\infty$ eine komplexe Bewertung ist, $\mathfrak{P}_\infty \mid \mathfrak{p}_\infty$, $\mathfrak{p}_\infty$ dagegen eine reelle, so sagt man, $\mathfrak{p}_\infty$ „verzweige" sich in K. Dann soll der Körper aller derjenigen Zahlen von K, denen bei der Bewertung $\mathfrak{P}_\infty$ reelle Werte zukommen, als der Trägheitskörper K_0 zu $\mathfrak{P}_\infty$ bezeichnet werden. Alle höheren Verzweigungskörper sollen mit K übereinstimmen:

$$\begin{aligned}k \leqq K_0 < K_1 &= K, \\ -1 = v_0 < v_1 &= 0, \\ n_0 > n_1 &= 1.\end{aligned}$$

In allen anderen Fällen, also falls $\mathfrak{P}_\infty$ und $\mathfrak{p}_\infty$ beide reell oder beide komplex, soll schon $K_0 = K$ sein (also $n_0 = 1$, $r = 0$) [5]).

[4]) Herbrand: Sur la théorie des groupes de ramification, Journ. de Math. **10** (1931). Vgl. HN § 7, insb. Fußnote [11]).

[5]) Der Zerlegungskörper zu $\mathfrak{P}_\infty$ soll übrigens mit K_0 übereinstimmen. Diese Festsetzung weicht etwas von der früheren, in Hasse: Klassenkörperbericht I a, oder in Artin: Theorie der L-Reihen, Abh. Hamb. Sem. 8 (1931) zugrundegelegten ab. Herr Prof. Artin hat später bemerkt, daß die hier angegebene Festsetzung in mancher Hinsicht zweckmäßiger ist.

Unter dieser Festsetzung erstreckt sich auch die Hassesche Normenresttheorie galoisscher Zahlkörper ohne weiteres auf unendliche Primstellen; insbesondere ist folgendes Resultat über den abelschen Fall gültig für alle Primstellen [6]):

Ist K/k abelsch, so wird der Exponent $[\mathfrak{f}_\mathfrak{p}(\Omega/k)]$ des $\mathfrak{p}$-Führers von Ω/k durch folgende Formel gegeben:

$$(5)\quad [\mathfrak{f}_\mathfrak{p}(\Omega/k)] = \frac{n_0}{n_0}(v_1 - v_0) + \frac{n_1}{n_0}(v_2 - v_1) + \cdots + \frac{n_{\tau-1}}{n_0}(v_\tau - v_{\tau-1}).$$

τ ist dabei die früher definierte Zahl, die Nummer des kleinsten K_i, der Ω enthält. Die Summe auf der rechten Seite bedeutet 0, wenn $\tau = 0$ ist. Insbesondere also:

$$(6)\quad [\mathfrak{f}_\mathfrak{p}(K/k)] = \frac{n_0}{n_0}(v_1 - v_0) + \frac{n_1}{n_0}(v_2 - v_1) + \cdots + \frac{n_{r-1}}{n_0}(v_r - v_{r-1}).$$

§ 2. Die Herbrandsche Formel.

In diesem Paragraphen sei K/k abelsch und $k \leqq \Omega \leqq K$. Im übrigen sollen die Bezeichnungen aus § 1 beibehalten werden.

Wir untersuchen, wie die Führer $\mathfrak{f}(K/k)$, $\mathfrak{f}(\Omega/k)$, $\mathfrak{f}(K/\Omega)$ unter sich verknüpft sind. Unsere Betrachtung sei zunächst auf eine Primstelle $\mathfrak{p}$ bezogen.

Die $\mathfrak{p}$-Führer $\mathfrak{f}_\mathfrak{p}(K/k)$ und $\mathfrak{f}_\mathfrak{p}(\Omega/k)$ sind schon durch die Formeln (5), (6) gegeben. Wir berechnen nun $\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)$. Nach (1), (2), (6) haben wir offenbar:

$$\begin{aligned}[\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)] &= \frac{\bar{n}_0}{\bar{n}_0}(\bar{v}_1 - \bar{v}_0) + \frac{\bar{n}_1}{\bar{n}_0}(\bar{v}_2 - \bar{v}_1) + \cdots + \frac{\bar{n}_{\bar{r}-1}}{\bar{n}_0}(\bar{v}_{\bar{r}} - \bar{v}_{\bar{r}-1}) \\ &= \frac{n'_0}{n'_0}(v_1 - v_0) + \frac{n'_1}{n'_0}(v_2 - v_1) + \cdots + \frac{n'_{\sigma-1}}{n'_0}(v_\sigma - v_{\sigma-1}).\end{aligned}$$

Nun unterscheiden wir zwei Fälle: I. $\tau < r$ und II. $\tau = r$.

I. $\tau < r$. Nach Definition von τ bedeutet diese Voraussetzung: $\Omega \leqq K_{r-1}$. Das zieht nach sich: $\sigma = r$, also $\tau < \sigma = r$. Denn dann kann offenbar $\Omega K_i = K$ für kein $i \leqq r-1$ bestehen. Übrigens ist unsere Voraussetzung auch mit

$$[\mathfrak{f}_\mathfrak{p}(\Omega/k)] < [\mathfrak{f}_\mathfrak{p}(K/k)] \quad \text{oder} \quad \mathfrak{f}_\mathfrak{p}(\Omega/k) < \mathfrak{f}_\mathfrak{p}(K/k)$$

äquivalent. (Wir verwenden die „Ungleichung" $\mathfrak{a} < \mathfrak{b}$ für Ideale $\mathfrak{a}, \mathfrak{b}$ in dem Sinne, daß $\mathfrak{a}$ ein *echter* Teiler von $\mathfrak{b}$ ist.)

$[\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)]$ ist dann weiter gleich

$$\begin{aligned}&\left\{\frac{n'_0}{n'_0}(v_1 - v_0) + \frac{n'_1}{n'_0}(v_2 - v_1) + \cdots + \frac{n'_{\tau-1}}{n'_0}(v_\tau - v_{\tau-1})\right\} + \cdots + \frac{n'_{r-1}}{n'_0}(v_r - v_{r-1}) \\ &\qquad = \{\varphi - \varphi_0\} + v_0\left[\frac{n_\tau}{n_0}(v_{\tau+1} - v_\tau) + \cdots + \frac{n_{r-1}}{n_0}(v_r - v_{r-1})\right]\end{aligned}$$

nach (2), (3), (4). Man beachte dabei, daß für $i \geqq \tau$ $\Omega K_i = K_i$, also $n'_i = n_i$ ist. Nach (5), (6) ist aber die Summe in der eckigen Klammer gleich

$$[\mathfrak{f}_\mathfrak{p}(K/k)] - [\mathfrak{f}_\mathfrak{p}(\Omega/k)].$$

v_0 ist ferner die Ordnungszahl von $\mathfrak{p}$ in $\bar{\mathfrak{p}}$. $\varphi - \varphi_0$ ist eine nur von Ω/k, und nicht von K abhängige Zahl. Setzt man also

$$(7)\quad \mathfrak{F}_{\bar{\mathfrak{p}}}(\Omega/k) = \bar{\mathfrak{p}}^{\varphi-\varphi_0},$$

$$(8)\quad \mathfrak{F}_\mathfrak{p}(\Omega/k) = \mathfrak{F}_{\bar{\mathfrak{p}}}(\Omega/k) \cdot \mathfrak{F}_{\bar{\mathfrak{p}}'}(\Omega/k) \cdots,\ \mathfrak{f}_\mathfrak{p}(K/\Omega) = \mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega) \cdot \mathfrak{f}_{\bar{\mathfrak{p}}'}(K/\Omega) \cdots,$$

so erhält man:

$$\mathfrak{f}_\mathfrak{p}(K/\Omega) \cdot \mathfrak{f}_\mathfrak{p}(\Omega/k) = \mathfrak{f}_\mathfrak{p}(K/k) \cdot \mathfrak{F}_\mathfrak{p}(\Omega/k).$$

---

[6]) Die Richtigkeit von (5), (6) für unendliche Primstellen ist übrigens durch direkte Verifizierung noch leichter zu bestätigen.

II. $\tau = r$. Dann gilt jedenfalls $\sigma \leqq \tau = r$ und

$$\mathfrak{f}_{\mathfrak{p}}(\Omega/k) = \mathfrak{f}_{\mathfrak{p}}(K/k)\,.$$

Aus der oben ausgeführten Berechnung von $\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)$ ergibt sich hier nur:

$$[\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)] \leqq \varphi - \varphi_0\,.$$

Führt man wie früher $\mathfrak{F}_{\bar{\mathfrak{p}}}(\Omega/k)$, $\mathfrak{F}_{\mathfrak{p}}(\Omega/k)$, $\mathfrak{f}_{\mathfrak{p}}(K/\Omega)$ gemäß (7), (8) ein, so erhält man:

$$\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega) \leqq \mathfrak{F}_{\bar{\mathfrak{p}}}(\Omega/k), \quad \mathfrak{f}_{\mathfrak{p}}(K/\Omega) \leqq \mathfrak{F}_{\mathfrak{p}}(\Omega/k)\,.$$

Der Exponent von $\bar{\mathfrak{p}}$ im Quotient der rechten Seite der ersteren Formel durch die linke ist gleich

$$c_{\bar{\mathfrak{p}}} = [\mathfrak{F}_{\bar{\mathfrak{p}}}(\Omega/k)] - [\mathfrak{f}_{\bar{\mathfrak{p}}}(K/\Omega)] = \frac{n'_\sigma}{n'_0}(v_{\sigma+1} - v_\sigma) + \cdots + \frac{n'_{\tau-1}}{n'_0}(v_\tau - v_{\tau-1})\,.$$

Nunmehr definieren wir für $\sigma > \tau$ von vornherein $c_{\bar{\mathfrak{p}}}$ als diese Summe; für $\sigma \leqq \tau$ soll $c_{\bar{\mathfrak{p}}} = 0$ sein. Setzt man dann

$$\mathfrak{C}_{\bar{\mathfrak{p}}} = \bar{\mathfrak{p}}^{c_{\bar{\mathfrak{p}}}}, \quad \mathfrak{C}_{\mathfrak{p}} = \mathfrak{C}_{\bar{\mathfrak{p}}}\mathfrak{C}_{\bar{\mathfrak{p}}'} \cdots,$$

so gilt

$$\mathfrak{C}_{\mathfrak{p}} \cdot \mathfrak{f}_{\mathfrak{p}}(K/\Omega) \cdot \mathfrak{f}_{\mathfrak{p}}(\Omega/k) = \mathfrak{F}_{\mathfrak{p}}(\Omega/k) \cdot \mathfrak{f}_{\mathfrak{p}}(K/k) \tag{9}$$

in voller Allgemeinheit (d. h. sowohl im Fall I als auch im Fall II).

Setzt man ferner:

$$\prod_{\mathfrak{p}} \mathfrak{F}_{\mathfrak{p}}(\Omega/k) = \mathfrak{F}(\Omega/k), \quad \prod_{\mathfrak{p}} \mathfrak{C}_{\mathfrak{p}} = \mathfrak{C} \quad \text{(Produkt über alle Primstellen)},$$

so ergibt sich die **Herbrandsche Formel**[7]):

$$\mathfrak{C} \cdot \mathfrak{f}(K/\Omega) \cdot \mathfrak{f}(\Omega/k) = \mathfrak{F}(\Omega/k) \cdot \mathfrak{f}(K/k)\,. \tag{10}$$

Von den Eigenschaften von $\mathfrak{C}$ ist folgendes zu vermerken:

$\mathfrak{C}$ ist ein ganzes Ideal in Ω, und $\mathfrak{C}_{\mathfrak{p}}$ ist sicher $= 1$, sobald $\mathfrak{f}_{\mathfrak{p}}(\Omega/k) < \mathfrak{f}_{\mathfrak{p}}(K/k)$ ist.[8]).

Das Ideal $\mathfrak{F}(\Omega/k)$ in Ω nenne ich aus später zu erläuternden Gründen den „Geschlechtermodul". Er ist nach (4) ein Teiler von $\mathfrak{f}(\Omega/k)$ und bleibt bei den Automorphismen von Ω/k invariant. (Entsprechendes gilt auch von $\mathfrak{F}_{\mathfrak{p}}(\Omega/k)$.)

Es möge hier noch ein Zusatz hinzugefügt werden: *Die Relationen*

(A) $$\mathfrak{f}(K/\Omega) \leqq \mathfrak{m} \cdot \mathfrak{F}(\Omega/k) \quad \textit{und}$$

(B) $$\mathfrak{f}(K/k) \leqq \mathfrak{m} \cdot \mathfrak{f}(\Omega/k)$$

bedingen sich gegenseitig, wenn $\mathfrak{m}$ irgendein ganzes Ideal in k ist.

Daß (A) aus (B) folgt, sieht man sofort aus Formel (10). Um das Umgekehrte zu beweisen, gehen wir indirekt vor.

Angenommen, (B) wäre nicht richtig, also

$$\mathfrak{f}(K/k) \nleqq \mathfrak{m} \cdot \mathfrak{f}(\Omega/k).$$

Dann gäbe es mindestens eine Stelle $\mathfrak{p}$, für die

$$\mathfrak{f}_{\mathfrak{p}}(K/k) > \mathfrak{m}_{\mathfrak{p}} \cdot \mathfrak{f}_{\mathfrak{p}}(\Omega/k)$$

---

[7]) HG § 1. Dort steht allerdings die Betrachtung bezüglich $\mathfrak{C}$ versehentlich aus. Das „lemme" Herbrands in der ursprünglichen Gestalt gilt z. B. im „Grenzfall" $\Omega = K$ nicht. Herbrand definiert ferner den Beitrag der unendlichen Primstellen anders wie wir, nämlich immer gleich 1. Der Tatbestand ist der, daß sich in der Formel (10) der unendliche Bestandteil von $\mathfrak{F}(\Omega/k)$ stets gegen den von $\mathfrak{C}$ völlig forthebt.

[8]) In meiner früheren Arbeit: Über den Wertvorrat des Normenrestsymbols, Abh. Hamb. Sem. **9** (1932), habe ich die den Verzweigungskörpern zugeordneten Idealgruppen in k explizit bestimmt (§ 2, a. a. O.). Danach könnte man eine Regel angeben, wie die Zahlen $c_{\bar{\mathfrak{p}}}$, mithin auch der Faktor $\mathfrak{C}$, im Grundkörper zu ermitteln sind. Darauf kommt es aber hier nicht weiter an.

gälte. Dann hätte man a fortiori $\mathfrak{f}_\mathfrak{p}(K/k) > \mathfrak{f}_\mathfrak{p}(\Omega/k)$, also $\mathfrak{C}_\mathfrak{p} = 1$. Aus der Formel (9) folgte dann:

$$\mathfrak{f}_\mathfrak{p}(K/\Omega) > \mathfrak{m}_\mathfrak{p} \cdot \mathfrak{F}_\mathfrak{p}(\Omega|k),$$

was mit (A) in Widerspruch stände [9]).

§ 3. Anwendungen.

1. Es sei Ω eine endliche, vorläufig sonst ganz beliebige Erweiterung von k, H eine Idealgruppe in k mit dem Führer $\mathfrak{m}$. Die Gesamtheit aller derjenigen Ideale in Ω, deren Normen nach k in H fallen, bildet eine Idealgruppe $\bar{H}$ in Ω, die sicher mod $\mathfrak{m}$ erklärbar ist. Der bekannte Begriff des „Hauptgeschlechtes" entsteht, wenn man für H spezielle Gruppen nimmt. Die Gruppe $\bar{H}$ möge also allgemein das „Hauptgeschlecht in Ω bezgl. H" heißen. Wenn speziell H der Strahl mod $\mathfrak{m}$ ist, so sagen wir statt „bezgl. H" auch einfacher „mod $\mathfrak{m}$". In der klassischen Theorie wird u. a. das Hauptgeschlecht mod $\mathfrak{f}(\Omega/k)$ für den Fall eines zyklischen Körpers Ω/k bestimmt.

Der Verschiebungssatz der Klassenkörpertheorie ermöglicht uns nun, die Frage nach der Bestimmung von $\bar{H}$ körpertheoretisch zu erfassen. Bildet man nämlich den Klassenkörper k' zu H über k und komponiert ihn mit Ω, so ist das Kompositum $K = \Omega k'$ nach dem genannten Satz gerade der Klassenkörper zu $\bar{H}$ über Ω. Insbesondere ist der Führer von $\bar{H}$ gleich $\mathfrak{f}(K/\Omega)$. Wenn Ω/k abelsch ist, so zeigt die Herbrandsche Formel, daß unter Umständen schon ein kleineres Ideal als $\mathfrak{m}$ als Erklärungsmodul von $\bar{H}$ ausreicht. Denn in diesem Fall ist $\mathfrak{f}(K/k)$ bekanntlich gleich dem kleinsten gemeinsamen Multiplum von $\mathfrak{m}$ und $\mathfrak{f}(\Omega/k)$, etwa $\mathfrak{m}_0 \cdot \mathfrak{f}(\Omega/k)$. Nach (10) folgt sodann:

$$\mathfrak{C} \cdot \mathfrak{f}(K/\Omega) = \mathfrak{m}_0 \cdot \mathfrak{F}(\Omega/k).$$

$\mathfrak{f}(K/\Omega)$ ist also ein Teiler von $(\mathfrak{m}, \mathfrak{m}_0 \cdot \mathfrak{F}(\Omega/k))$. Insbesondere ist das Hauptgeschlecht mod $\mathfrak{f}(\Omega/k)$ sicher mod $\mathfrak{F}(\Omega/k)$ erklärbar; daher die Benennung „Geschlechtermodul" für $\mathfrak{F}(\Omega/k)$.

2. Denken wir uns umgekehrt, eine Idealgruppe $\bar{H}_*$ mod $\mathfrak{M}$ sei im Oberkörper Ω vorgegeben. Dann definieren wir die „Norm von $\bar{H}_*$ nach k" folgendermaßen:

Sei zunächst $\mathfrak{m}$ irgendein Multiplum von $\mathfrak{M}$ in k. Die Gesamtheit der Strahlklassen mod $\mathfrak{m}$, in die die Normen der Ideale aus $\bar{H}_*$ fallen, bilden eine Idealgruppe $H_\mathfrak{m}$ mod $\mathfrak{m}$ in k. Sie soll die „Norm von $\bar{H}_*$ mod $\mathfrak{m}$" heißen. Ist K^* der Klassenkörper zu $\bar{H}_*$ über Ω, so ist $H_\mathfrak{m}$ ersichtlich dieselbe Idealgruppe in k, die K^* mod $\mathfrak{m}$ zugeordnet ist. Wählen wir also $\mathfrak{m}$ „groß genug", so wird sie mit der „zu K^* zugeordnete Idealgruppe in k" überhaupt übereinstimmen. Diese nunmehr von $\mathfrak{m}$ unabhängig gewordene Gruppe H wollen wir die „Norm von $\bar{H}_*$ nach k" nennen. (Sie ist also der Durchschnitt aller $H_\mathfrak{m}$.) In Zeichen:

$$N_{\Omega/k}(\bar{H}_*) = H. \tag{11}$$

Das Hauptgeschlecht $\bar{H}$ in Ω bezgl. H ist offenbar eine Obergruppe von $\bar{H}_*$. Es ist ferner klar, daß aus $\bar{H}_* \leqq \bar{H}_1$ $N_{\Omega/k}(\bar{H}_*) \leqq N_{\Omega/k}(\bar{H}_1)$ folgt.

In der ursprünglichen Geschlechtertheorie der zyklischen Körper geht man bekanntlich von der Gruppe aller Hauptideale in Ω als $\bar{H}_*$ aus. (Dann hat die Gruppe $H = N_{\Omega/k}(\bar{H}_*)$ übrigens $\mathfrak{f}(\Omega/k)$ als Führer.) Die Bedeutung der Relation (11) in der

[9]) Dieser letzte Schluß wurde in IH nicht klar dargelegt.

allgemeineren Theorie wird der folgende Absatz aufklären. Hier beweisen wir noch folgende Tatsache:

Ist Ω/k abelsch, $\mathfrak{m}$ irgendein ganzes Ideal in k, und

$$\bar{S}_* = \text{Strahl mod. } \mathfrak{m}\cdot\mathfrak{F}(\Omega/k), \quad S = \text{Strahl mod. } \mathfrak{m}\cdot\mathfrak{f}(\Omega/k),$$

so gilt

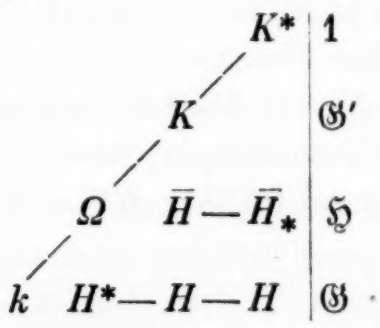
$$N_{\Omega/k}(\bar{S}_*) = S. \tag{12}$$

(Zur Abkürzung wollen wir dafür auch $N(\bar{S}_*) = S$ schreiben.)

1. Es sei K der Strahlklassenkörper mod $\mathfrak{m}\cdot\mathfrak{f}(\Omega/k)$, d. h. der Klassenkörper zu S über k. Ω ist dann offenbar in K enthalten, und das Hauptgeschlecht $\bar{S}$ in Ω mod $\mathfrak{m}\cdot\mathfrak{f}(\Omega/k)$, d. h. bezgl. S, ist, nach den im vorigen Absatz ausgeführten Schlüssen und dem Verschiebungssatz, gerade die dem Körper K zugeordnete Idealgruppe in Ω. Der Führer von $\bar{S}$ ist also $\mathfrak{f}(K/\Omega)$, und dieser ist nach dem Zusatz in § 2 [$(B) \to (A)$] ein Teiler von $\mathfrak{m}\cdot\mathfrak{F}(\Omega/k)$. Also ist $\bar{S}_* \leqq \bar{S}$, $N(\bar{S}_*) \leqq N(\bar{S}) = S$.

2. Es sei K^* der Strahlklassenkörper mod $\mathfrak{m}\cdot\mathfrak{F}(\Omega/k)$, d. h. der Klassenkörper zu $\bar{S}_*$ über Ω, und K_1 der größte über k abelsche Teilkörper von K^*/k. Es gilt dann offenbar $K^* \geqq K_1 \geqq \Omega$. Die Idealgruppe $N(\bar{S}_*)$ ist dann ersichtlich diejenige Gruppe in k, die dem Körper K^* zugeordnet ist. Nach dem Abgrenzungssatz der Klassenkörpertheorie ist sie aber identisch mit der dem Körper K_1 zugeordneten Gruppe. Nun ist der Führer von K_1/Ω ein Teiler von $\mathfrak{f}(K^*/\Omega) = \mathfrak{m}\cdot\mathfrak{F}(\Omega/k)$, da ja $K^* \geqq K_1 \geqq \Omega$, wie schon vermerkt wurde. Daraus folgt nach dem Zusatz in § 2 [$(A) \to (B)$], daß der Führer von K_1/k, d. i. der Führer der Idealgruppe $N(\bar{S}_*)$, ein Teiler von $\mathfrak{m}\cdot\mathfrak{f}(\Omega/k)$ ist. Also ist $N(\bar{S}_*) \geqq S$.

3. Nunmehr sei Ω/k abelsch; H^* die zu Ω zugeordnete Gruppe in k; H eine in H^* enthaltene Idealgruppe. Ferner sei $\bar{H}_*$ eine bei den Automorphismen von Ω/k invariante Idealgruppe in Ω, die (11) genügt.



$\bar{H}$ bedeute wie früher das Hauptgeschlecht in Ω bezgl. H. Für den Fall, daß Ω/k zyklisch ist, beantwortet die klassische Theorie die Frage: „Welche Klassen nach $\bar{H}_*$ gehören zu $\bar{H}$?“ in folgenden Spezialfällen [10]):

1. $\bar{H}_* =$ Gruppe aller Hauptideale in Ω, $H = N_{\Omega/k}(\bar{H}_*)$.
2. $\bar{H}_* =$ Strahl mod $\mathfrak{m}\cdot\mathfrak{F}(\Omega/k)$, $H =$ Strahl mod $\mathfrak{m}\cdot\mathfrak{f}(\Omega/k)$.

(Wir haben eben bewiesen, daß auch im Falle 2. die Voraussetzung (11) $N(\bar{H}_*) = H$ erfüllt ist. Daß auch die anderen Bedingungen in beiden Fällen befriedigt sind, bedarf

---

[10]) Der Inhalt der Absätze **3**, **4** ist von der Theorie der Führer bzw. der Geschlechtermoduln unabhängig.

Im Fall 2. stimmen aber die Körper K, K^*, K_1 dieses Absatzes **3**, wie sofort ersichtlich, bzw. mit den gleichbezeichneten Körpern im vorigen Absatz **2** überein. Bei direkter Behandlung dieses Falls kann man also den Beweis kürzer fassen, indem man die Schlüsse in **2** in das Beweisschema von **3** hineinschiebt, wie es ja auch schon in HG, IH geschehen ist. Hier wollten wir jedoch lieber den führertheoretischen Teil von dem übrigen Teil des Beweises absondern.

keines Beweises.) Hier wollen wir die Möglichkeit zeigen, die oben formulierte Frage unter unseren allgemeineren Voraussetzungen gruppentheoretisch zu behandeln.

Dazu bilden wir den Klassenkörper K zu H über k, und den Klassenkörper K^* zu $\bar{H}_*$ über Ω. Da $H^* \geqq H$, $\bar{H} \geqq \bar{H}_*$, folgt $\Omega \leqq K$, $K \leqq K^*$. Wegen der Invarianz von $\bar{H}_*$ bei den Automorphismen von Ω/k, ist ferner K^*/k galoissch. Es sei $\mathfrak{G}$ die galoissche Gruppe; $\mathfrak{H}$, $\mathfrak{G}'$ bzw. die Ω, K entsprechenden Untergruppen von $\mathfrak{G}$. Nach dem Artinschen Reziprozitätsgesetz wird die Gruppe der Klassen nach $\bar{H}_*$ in Ω auf die Gruppe $\mathfrak{H}$ isomorph abgebildet. Die Obergruppe $\bar{H}$ von $\bar{H}_*$ ist, wie wir schon mehrmals gesehen haben, die dem Körper K zugeordnete Idealgruppe in Ω. Diese Gruppe H entspricht also, als Untergruppe der Klassengruppe nach $\bar{H}_*$ aufgefaßt, bei der Zuordnung: Klasse nach $\bar{H}_* \longleftrightarrow$ Element von $\mathfrak{H}$, genau der Untergruppe $\mathfrak{G}'$ von $\mathfrak{G}$. Wir haben nun diese Gruppe $\mathfrak{G}'$ gruppentheoretisch zu charakterisieren. Sie ist die Kommutatorgruppe von $\mathfrak{G}$.

Das beweisen wir wieder körpertheoretisch; wir zeigen nämlich, daß K mit dem größten über k abelschen Teilkörper K_1 von K^*/k übereinstimmt.

K_1 enthält zunächst Ω, also gilt $K^* \geqq K_1 \geqq \Omega$. Die zu K_1 zugeordneten Idealgruppen in k, Ω sollen bzw. H_1, $\bar{H}_1$ genannt werden. Wegen $K^* \geqq K_1$ gilt $\bar{H}_* \leqq \bar{H}_1$, folglich $H = N_{\Omega/k}(\bar{H}_*) \leqq N_{\Omega/k}(\bar{H}_1) = H_1$, $K \geqq K_1$. Aus der vorausgesetzten Maximalität von K_1 folgt sodann $K = K_1$, w. z. b. w.

4. Wir führen schließlich noch die Annahme ein, daß die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, d. h. die Gruppe von Ω/k, zyklisch sei. Es sei σ ein Element von $\mathfrak{G}$, so daß $\sigma\mathfrak{H}$ diese Faktorgruppen erzeugt.

Wir bezeichnen die Klassen nach $\bar{H}_*$ allgemein mit C. σ bewirkt einen Automorphismus für diese Klassen: $C \to C^\sigma$. Ist γ das Bildelement von C in $\mathfrak{H}$, so entspricht der Klasse C^σ bekanntlich $\sigma\gamma\sigma^{-1}$. Wir wollen dementsprechend für $\sigma\gamma\sigma^{-1}$ auch γ^σ schreiben. Die Elemente der Kommutatorgruppe sind aber im vorliegenden Fall offenbar in der Gestalt $\sigma\gamma\sigma^{-1}\gamma^{-1} = \gamma^{\sigma-1}$ darstellbar. Das bedeutet: *Unter den Klassen nach $\bar{H}^*$ gehören alle und nur die zum Hauptgeschlecht $\bar{H}$, die sich als $(1 - \sigma)$-te Potenz einer Klasse schreiben lassen.* Die bekannten Sätze über Geschlechter sind Spezialfälle dieses Satzes.

5. In der Betrachtung im Absatz **3** setze man speziell:

Ω = Strahlklassenkörper, also

H^* = Strahl mod $\mathfrak{f}(\Omega/k)$, $H^* = H$, und

$\bar{H}_*$ = Strahl mod $\mathfrak{F}(\Omega/k)$, was wegen (12) erlaubt ist.

Dann bekommt man $\Omega = K$, $\mathfrak{H} = \mathfrak{G}'$; d. h. dem Körper Ω selbst, als Teilkörper von K^*/k, entspricht die Kommutatorgruppe. Aus dem Furtwänglerschen Satz über metabelsche Gruppen folgt somit der allgemeine Hauptidealsatz: *Alle Ideale des Grundkörpers fallen im Strahlklassenkörper in den Strahl modulo dem Geschlechtermodul.*

Noch mehrere Sätze über metabelsche Gruppe können auf diese Weise arithmetisch gedeutet werden. Man kann ferner die oben immer „im Großen" gemachten Schlüsse natürlich auch „lokal" durchführen, oder aber, statt des Strahlklassenkörpers den l-Strahlklassenkörper, d. h. den größten Klassenkörper mit einem gegebenen Modul, dessen Grad gleich einer Potenz einer vorgegebenen Primzahl l ist, betrachten, und so weitere Sätze herleiten. Darauf soll jedoch hier nicht näher eingegangen werden.

Eingegangen 20. Mai 1933.

Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm.

Von *A. Scholz* in Freiburg und *O. Taussky* in Wien.

E. Artin hat gezeigt, daß es möglich ist, mit Hilfe der Beweismethoden für den Hauptidealsatz der Klassenkörpertheorie auch Aussagen darüber zu gewinnen, wie die Klassen eines algebraischen Zahlkörpers allmählich in den Unterkörpern des Klassenkörpers in die Hauptklasse übergehen. Die Gesetze, nach denen sich dieses Hauptidealwerden vollzieht, sind aber nur teilweise bekannt und wahrscheinlich von ziemlich komplizierter Natur.

Es ist bekannt, daß nicht allgemein ein eineindeutiges Entsprechen zwischen den Unterkörpern des Klassenkörpers und den Untergruppen der Klassengruppe, welche in ihnen zur Hauptklasse werden, besteht. Das gilt nur in ganz speziellen Fällen. Insbesondere kann die Anzahl der Klassen, welche in einem echten Unterkörper des Klassenkörpers zur Hauptklasse werden, größer sein als der Relativgrad des Körpers. Es kann sogar eintreten, daß sämtliche Klassen bereits in einem echten Unterkörper des Klassenkörpers in die Hauptklasse übergehen. Dagegen kann man zeigen, daß nicht jede Klasse bereits in einem echten Unterkörper des Klassenkörpers Hauptideal werden muß. Ferner weiß man zwar, daß in jedem relativ-zyklischen Zwischenkörper mindestens eine Untergruppe der Klassengruppe zur Hauptklasse werden muß, welche dieselbe Ordnung hat wie der Relativgrad des Körpers. Doch braucht diese Untergruppe nicht zyklisch zu sein. Als Beispiel dafür ist von Artin und Furtwängler (siehe Hasse, Bericht II, S. 173) der Körper $P(\sqrt{-65})$ angegeben worden, welcher eine zweibasige Klassengruppe der Ordnung 8 besitzt. In Kapitel 1 wird der analoge Fall für ungerade Ordnungen der Klassengruppe untersucht, und zwar beim Körper $P(\sqrt{-3299})$, welcher der imaginär-quadratische Körper kleinster Diskriminante ist, der eine zweibasige Klassengruppe von ungerader Primzahlpotenzordnung besitzt. Dann wird an mehreren Beispielen gezeigt, wie vielfältig die Möglichkeiten bereits bei den einfachsten nicht zyklischen Klassengruppen von ungerader Primzahlpotenzordnung, nämlich beim Typus (3, 3) sind. Diese Untersuchungen benützen das Artinsche Reziprozitätsgesetz nicht. *Es wird mit Hilfe von Relationen im Körper der rationalen Zahlen entschieden*, welche Klassen in den relativ unverzweigten kubischen Oberkörpern zur Hauptklasse werden. Für diesen Abschnitt waren die Sätze von Hasse über kubische Körper (Math. Zeitschrift 31) sehr wichtig.

In Kapitel 2 wird gezeigt, wie weit man von dem Hauptidealwerden in den Zwischenkörpern auf die Relativgruppe des zweiten Klassenkörpers, insbesondere auf die Klassengruppe des Klassenkörpers schließen kann. Es ergibt sich, daß diese Relativgruppe mitunter durch das Hauptidealwerden in den Zwischenkörpern bereits eindeutig festgelegt ist.

In Kapitel 3 wird — wie in Kapitel 2 — mit rein gruppentheoretischen Hilfsmitteln bewiesen, daß der 3-Klassenkörperturm aller behandelten Körper und einer umfangreichen Klasse weiterer Körper, deren Klassengruppe vom Typus $(3^{n_1}, 3^{n_2})$ ist, genau zweistufig ist. Das Hauptidealwerden in den Unterkörpern des absoluten Klassenkörpers bestimmt also oft schon die Ausdehnung und Struktur des ganzen Klassenkörperturms.

1. Die Bestimmung der Hauptideale in den kubischen Klassenkörpern.

Gegeben seien die imaginär-quadratischen Zahlkörper $\mathsf{P}(\sqrt{-4027})$, $\mathsf{P}(\sqrt{-9748})$ und $\mathsf{P}(\sqrt{-3299})$ mit den Klassenzahlen 9, 18, 27. Für keinen der Körper ist die Klassengruppe zyklisch, und zwar ist die 3-Klassengruppe in den ersten beiden Fällen vom Typ (3, 3), im letzten Fall vom Typ (3, 9). Es sollen für jeden der drei Körper $\mathsf{P}(\sqrt{D})$ die Idealklassen bestimmt werden, die in den verschiedenen kubischen Unterkörpern des absoluten Klassenkörpers von $\mathsf{P}(\sqrt{D})$ in die Hauptklasse übergehen.

Wir geben zuerst die allgemeine Methode an und führen sie dann für die drei gegebenen $\mathsf{P}(\sqrt{D})$ durch.

Um erst einmal die Klassenzahl von $K_0 = \mathsf{P}(\sqrt{D})$ zu bestimmen, stellen wir nach bekannter Methode die reduzierten quadratischen Formen (a, b, c) der Diskriminante D auf und bekommen auf diese Weise für jede Idealklasse des Körpers $\mathsf{P}(\sqrt{D})$ ein Ideal $\left(a, \frac{b+\sqrt{D}}{2}\right)$ als Repräsentanten. Da die 3-Klassengruppe zwei Basisklassen C_1, C_2 besitzt, enthält sie genau vier Untergruppen vom Index 3, nämlich

$$H_1 = H_0 + H_0C_1 + H_0C_1^2 \qquad H_2 = H_0 + H_0C_2 + H_0C_2^2$$
$$H_3 = H_0 + H_0C_1C_2 + H_0C_1^2C_2^2 \qquad H_4 = H_0 + H_0C_1C_2^2 + H_0C_1^2C_2,$$

wo H_0 der Hauptklassenverband, die Untergruppe der dritten Potenzklassen ist. Daher gibt es über $K_0 = \mathsf{P}(\sqrt{D})$ vier unverzweigte kubische Oberkörper K_1, K_2, K_3, K_4. Für diese können wir in P vier kubische Gleichungen $F(x) = 0$ bestimmen, so daß $K = K_0(\vartheta) = \mathsf{P}(\sqrt{D}, \vartheta)$ wird, wenn ϑ eine Wurzel von $F(x) = 0$ ist, und $\mathsf{P}(\vartheta)$ die Diskriminante D hat [1]). Diese vier Körper K oder deren absolut kubische Unterkörper $\mathsf{P}(\vartheta)$ ordnen sich bekanntlich obigen vier Untergruppen H_i so zu, daß die Primideale aus H_i und nur diese in K voll zerfallen [1]). Bezeichnet man die entsprechenden quadratischen Formenklassenverbände mit denselben Buchstaben, so hat man das rationale Kriterium für die Zuordnung $F(x) \to H_i$: Geht die rationale Primzahl p nicht in der Diskriminante von $F(x)$ auf, so zerfällt $F(x)$ mod p dann und nur dann in Linearfaktoren, wenn p in H_i darstellbar ist. Wir suchen nun für jedes H_i eine Primzahl p_i, die sich in H_i, aber nicht in H_0 darstellen läßt. Diese zerfällt dann nur in dem einen, zu H_i gehörigen Klassenkörper K, den wir jetzt mit K_{p_i} bezeichnen wollen, ebenso mit $F_{p_i} = 0$ die zugehörige Gleichung [1] [1a]).

Sodann schreiten wir zur eigentlichen Aufgabe: zu bestimmen, welche Klassen von K_0 in den einzelnen K_{p_i} in die Hauptklasse übergehen („kapitulieren"). Diese Aufgabe läßt sich folgendermaßen auf eine rationale Gestalt bringen: Ist $\mathfrak{j}$ ein Ideal aus K_0, das etwa in $K = K_{p_i} = K_0(\vartheta)$ Hauptideal wird: $\mathfrak{j} = (\gamma)$, so ist $\gamma^{S-1} = \varepsilon$ (die) Grundeinheit in K, wenn S die erzeugende Substitution von K/K_0 ist [2]). Es ist dann $\mathfrak{j}^3 = (\alpha)$

[1]) Vgl. H. Hasse, Math. Z. **31** (1930), 565—582.

[1a]) Anmerkungen in eckigen Klammern befinden sich am Schluß des 1. Kapitels.

[2]) Vgl. Hilbert, Zahlbericht § 58. Ges. Abh. Bd. 1, S. 155—156.

in K_0, wo

$$\alpha = N_{K_0}(\gamma) = \gamma^{1+S+S^2} = \gamma^{(S-1)^2+3S} = \varepsilon^{S-1}\gamma^{3S}.$$

Ist nun $q = 3n + 1$ eine in K voll zerfallende Primzahl, für die ε^{S-1} kubischer Rest ist, so ist auch $\alpha = \varepsilon^{S-1}\gamma^{3S}$ kubischer Rest mod q, und umgekehrt. Repräsentieren die Ideale $\mathfrak{j}$ und $\mathfrak{f}$ eine Basis für die Idealklassen der Ordnung 3, und ist der oben gewählte Modul q so beschaffen, daß nur $\mathfrak{j}^3$, aber nicht $\mathfrak{f}^3$ kubischer Rest mod q ist, so steht jetzt fest, daß gerade die Idealklasse von $\mathfrak{j}$ mit ihrer Inversen in K kapituliert.

Zur Lösung unserer Aufgabe ist also erstens zu jedem Paar inverser Idealklassen der Ordnung 3 in K_0 ein $\alpha = \mathfrak{j}^3$ zu bestimmen, wo $\mathfrak{j}$ einer solchen Klasse angehört. Durch Normbildung $N(\mathfrak{j}) = c$, $N(\alpha) = c^3$, wird die Aufgabe rational, d. h. die Darstellung von $4c^3 = x^2 + |D|\,y^2$ führt zu $\alpha = \dfrac{x + y\sqrt{D}}{2}$, wenn man c vorher so gewählt hat, daß es in dem betreffenden Formenklassenpaar, aber keiner anderen Klasse der Ordnung 3 oder der Hauptklasse darstellbar ist (vorzugsweise also als Primzahl).

Zweitens ist in jedem der vier kubischen Körper K eine Grundeinheit oder $(S-1)$-te Potenz einer solchen zu bestimmen, und dann ein passender Modul q obengenannter Art, für den aber außerdem nicht gerade alle vier Werte α (sondern nur einer) kubischer Rest ist. Das Aufsuchen einer passenden Einheit wird im allgemeinen das schwierigste sein. Man kann sich aber die Aufgabe in zweierlei Hinsicht vereinfachen: einmal kann man die Einheit aus dem absolut kubischen Körper $\mathsf{P}(\vartheta)$ entnehmen; denn ist sie dort nicht gerade Einheitskubus, so auch nicht in $K_0(\vartheta)$, also dort keine $(S-1)^2$-te, sondern höchstens $(S-1)$-te Potenz einer Einheit [2]. Weiter darf man im Hinblick auf den passenden Modul q die Grundeinheit oder deren $(S-1)$-te Potenz noch mit einer beliebigen dritten Zahlpotenz multiplizieren (die Grundeinheit sogar außerdem mit irgendeiner rationalen Zahl), ohne daß am Restcharakter von $\alpha = \varepsilon^{S-1}\gamma^{3S}$ etwas geändert wird; statt einer Einheit brauchen wir also nur ein $\sigma = \varepsilon\tau^3$.

Um nun noch ein passendes q zu bestimmen, das für die Kapitulation entscheidend ist, muß man vor allem wissen, ob für das gefundene ε oder $\sigma = \varepsilon\tau^3$ wirklich ε Grundeinheit oder $(S-1)$-te Potenz einer solchen ist. Für den Fall der Grundeinheit ε gibt es immer Primzahlen $r = 3n + 1$, die in $\mathsf{P}(\vartheta)$ voll zerfallen, und für die ε nur $(3, S-1)$-ter ($\mathfrak{L}$-ter), aber kein $(3, (S-1)^2)$-ter ($\mathfrak{L}_2$-ter) Potenzrest ist, also $\varepsilon \equiv \xi^{S-1}\eta^3$, aber $\not\equiv \xi^{(S-1)^2}\eta^3$ (mod r). Die $\mathfrak{L}_2$-ten Potenzreste sind nun diejenigen, deren $(S-1)$-te Potenz kubischer Rest ist. Da aber ε^{S-1} kein Zahlkubus ist, so muß es Primzahlen r der obengenannten Eigenschaft geben (und diese besitzen unter den voll zerfallenden $p = 3n + 1$ die Dichte 2/3; $\mathfrak{L}$-ter Potenzrest ist ε wegen $\varepsilon^{1+S+S^2} = 1$ immer). — Hat man umgekehrt ein r gefunden, für das ε oder σ (s. o.) nur $\mathfrak{L}$-ter, aber nicht $\mathfrak{L}_2$-ter Potenzrest ist, und ein q, für das es $\mathfrak{L}_2$-ter Rest ist, so ist ε Grundeinheit, und es gilt für das in $K_0(\vartheta)$ kapitulierende $\mathfrak{j} = (\gamma)$: $\alpha = \mathfrak{j}^3 = N_{K_0}(\gamma)$ ist kubischer Rest mod q. Hat man aber nur ein r gefunden, für das ε schon $\mathfrak{L}_2$-ter, aber nicht kubischer Rest ist, so reicht ein q, für das ε kubischer Rest ist; denn in diesem Fall kann ε höchstens $(S-1)$-te Potenz der Grundeinheit sein. — Ob ε nun $\mathfrak{L}$-ter, $\mathfrak{L}_2$-ter oder kubischer Rest mod p ist, entscheidet man am einfachsten durch den kubischen Restcharakter von ε nach den drei Primteilern von p: $\mathfrak{L}_2$-te Reste sind diejenigen, die nach den drei Primteilern den gleichen kubischen Restcharakter aufweisen, da aus ihrer Potenzierung mit $S-1$ die kubischen Reste hervorgehen. Nur $\mathfrak{L}$-te Potenzreste sind diejenigen, die nach allen drei Primteilern verschiedene Restcharaktere besitzen, da aus ihrer Potenzierung diejenigen $\mathfrak{L}_2$-ten Reste hervorgehen, welche nicht kubische Reste sind. Bezeichnet ϱ die dritte Einheitswurzel, und wird der Restcharakter etwa des kleinsten kubischen Nichtrestes als ϱ fest-

gelegt, so gilt:

Restcharakter $\chi(\varepsilon)$	$1, \varrho, \varrho^2$	$\varrho, \varrho, \varrho$	$1, 1, 1$
ε Potenzrest	$\mathfrak{L}$-ter	$\mathfrak{L}_2$-ter	3-ter

(Bei $\mathfrak{L}$-tem Potenzrest kommt natürlich je nach der Reihenfolge der Primteiler von p irgendeine Permutation von $1, \varrho, \varrho^2$ vor, und bei $\mathfrak{L}_2$-tem Rest auch $\varrho^2, \varrho^2, \varrho^2$.)

Hat man auf diese Weise ein q bestimmt, für das die Grundeinheit schon $\mathfrak{L}_2$-ter Rest ist, so kann es, wie schon oben bemerkt, immer noch eintreten, daß alle vier $\alpha = \mathfrak{j}^3$ kubische Reste mod q sind. Diese $q = q^*$ (deren Primteiler in $K_0(\sqrt{-3}, \vartheta)$ die primären Primideale sind) haben aber unter allen voll zerfallenden p nur die Dichte 1/9 (je 2/9 dagegen die, für die nur ein bestimmtes der vier α kubischer Rest wird), also unter den oben zugelassenen q die Dichte 1/3 [3]. Die wirklich entscheidenden q haben also unter den p immer noch die Dichte 2/9, und daher wird die Bestimmung von q im allgemeinen nicht viel Proben erfordern.

Wir bringen nun die Beispiele.

I. $D = -4027$.

Reduzierte Formen.	Zugehörige Gleichungen.	Diskriminante.	Körper.
$(1, 1, 1007)$			
$(19, \pm 1, 53)$	$F_{19}(x) = x^3 + 43x - 56 = 0$	$\Delta = 100D$	K_{19}
$(13, + 9, 79)$	$F_{13}(x) = x^3 - 44x - 113 = 0$	$\Delta = D$	K_{13}
$(17, \pm 11, 61)$	$F_{17}(x) = x^3 - 8x - 15 = 0$	$\Delta = D$	K_{17}
$(29, \pm 27, 41)$	$F_{29}(x) = x^3 + 10x - 1 = 0$	$\Delta = D$	K_{29}.

Idealkuben $\mathfrak{j}^3 = \alpha$:

$$\mathfrak{j}_{19}^3 = \frac{153 + \sqrt{D}}{2}, \quad \mathfrak{j}_{13}^3 = \frac{69 + \sqrt{D}}{2}, \quad \mathfrak{j}_{17}^3 = \frac{125 + \sqrt{D}}{2}, \quad \mathfrak{j}_{29}^3 = 91 + 2\sqrt{D}.$$

Wir gehen jetzt der Reihe nach die vier Körper durch, die wir in der Rechnung mit [19], [13], [17], [29] notieren, und betrachten den Kongruenzzerfall der zugehörigen Gleichung nach passenden Primzahlen $p = 3n + 1$, die in den betreffenden Untergruppen der Formenklassen darstellbar sind, in der Rechnung durch (p) notiert. Wir setzen immer $\chi(w) = \langle w \rangle = \varrho$ für den kleinsten kubischen Nichtrest, und auch sonst gebrauchen wir $\langle a \rangle$ als Abkürzung für $\chi(a)$.

[29] $\quad F(x) = x^3 + 10x - 1 = 0.$

ϑ ist Einheit.

(43) $\quad \vartheta \equiv -12, -15, -16$ nach den verschiedenen Primteilern von 43.

Da 16 kubischer Rest mod 43, aber nicht 12 und 15, so folgt, daß ϑ Grundeinheit ist.

(103) $\quad \dfrac{\vartheta \equiv 4, 7, -11}{\langle \vartheta \rangle = \varrho^2, \varrho^2, \varrho^2}$ $\quad \langle 3 \rangle = \langle 100 \rangle = \langle 10 \rangle = 1; \ \langle 2 \rangle = \varrho; \ \langle 5 \rangle = \varrho^2 = \begin{cases} \langle 7 \rangle = \langle 96 \rangle \\ \langle 11 \rangle = \langle \frac{1}{2}\frac{2}{2}\frac{5}{2} \rangle \end{cases}$

weil $103 = x^2 + xy + 61y^2$ darstellbar.

Also ist 103 als Modul q brauchbar, wenn unter $\mathfrak{j}_{13}^3, \mathfrak{j}_{17}^3, \mathfrak{j}_{19}^3, \mathfrak{j}_{29}^3$ nur ein kubischer Rest ist — wozu die Feststellung eines Nichtkubus genügt. Nun ist $\sqrt{D} \equiv \pm 14$ nach den beiden Primteilern von 103 in K_0, also

$$\mathfrak{j}_{19}^3 \equiv 25 \pm 7; \quad \text{Rechtscharakter } \chi = \varrho^2, \varrho.$$

Dagegen

$$\mathfrak{j}_{13}^3 \equiv -17 \pm 7; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{13}$ in K_{29} Hauptideal.

$$[17] \qquad F(x) = x^3 - 8x - 15 = 0.$$

$$\eta = 7 - 2\vartheta \quad \text{ist Einheit.}$$

(61) $\vartheta \equiv -6, -12, 18$

$\eta \equiv 19, 31, 32$

$\langle\eta\rangle = \varrho^2, \varrho^2, \varrho^2$

$\langle 3\rangle = 1;\ \langle 2\rangle = \langle 5\rangle = \langle 7\rangle = \varrho.$

(67) $\vartheta \equiv 16, -15/2, -17/2$

$7 - 2\vartheta \equiv -25, 22, 24$

$\langle 7 - 2\vartheta\rangle = 1, 1, 1$

$\langle 3\rangle = 1;\ \langle 2\rangle = \varrho;\ \langle 5\rangle = \langle 72\rangle = 1;$
$\langle 11\rangle = \langle 56\rangle = \langle 7\rangle = \langle 60\rangle = \varrho^2.$

Wir können also $q = 67$ wählen. Es ist $\sqrt{D} \equiv \pm 23 \bmod q$.

$$\mathfrak{j}_{13}^3 \equiv 1 \pm 22;\ \chi = \varrho, \varrho^2.$$

Dagegen

$$\mathfrak{j}_{29}^3 \equiv 24 \pm 21;\quad \chi = 1.$$

Also wird $\mathfrak{j}_{29}$ in K_{17} Hauptideal.

$$[13] \qquad F(x) = x^3 - 44x - 113 = 0.$$

$$4 + \vartheta \quad \text{ist Einheit.}$$

(13) $\vartheta \equiv 1, 5, -6$

$4 + \vartheta \equiv 5, 9, -2$

$\langle 4 + \vartheta\rangle = 1, \varrho^2, \varrho$

(223) $\vartheta \equiv -9, -67, 76$

$\varepsilon \equiv -5, -63, 80$

$\langle\varepsilon\rangle = \varrho^2, \varrho^2, \varrho^2$

$\langle 2\rangle = \langle 7\rangle = \langle 13\rangle = 1.$
$\langle 3\rangle = \varrho.\ \langle 5\rangle = \langle 11\rangle = \varrho^2.$

$\varepsilon = 4 + \vartheta$ ist Grundeinheit. Wir können $q = 223$ setzen. Es ist $\sqrt{D} \equiv \pm 87$;

$$\mathfrak{j}_{13}^3 \equiv 78, -9;\quad \chi = \varrho, \varrho^2.$$

Dagegen

$$\mathfrak{j}_{19}^3 \equiv 120, 33;\quad \chi = 1.$$

Also wird $\mathfrak{j}_{19}$ in K_{13} Hauptideal.

$$[19] \qquad F(x) = x^3 + 43x - 56 = 0.$$

Die Gleichungsdiskriminante ist hier $\Delta = 100\,D$; es müssen also noch 2 und 5 als außerwesentliche Diskriminantenteiler nachgewiesen werden; erst dann haben wir die Gewißheit, daß $F(x)$ den Körper K_{19} bestimmt, weil $F(x)$ mod 19 voll zerfällt. Eine Einheit von der Form $x + y\vartheta$, wie wir sie bei den obigen drei Körpern hatten, scheint hier schwer auffindbar zu sein, und nach den Resultaten von Thue [3]) existieren auch immer nur endlich viele dieser Art — wenn überhaupt welche. In komplizierteren Fällen wäre man daher genötigt, die Einheit in der allgemeinen Form $\varepsilon = x + y\vartheta + z\vartheta^2$ zu suchen. Diese Methode ist aber praktisch fast unbrauchbar, da es schwer ist, x, y und z so gegeneinander abzustimmen, daß $N(\varepsilon) = \pm 1$ wird, während für $\varepsilon = x + y\vartheta$ einfach $N(\varepsilon) = x^3 - sxy^2 + ty^3 = \pm 1$ zu lösen ist, wenn ϑ der Gleichung $x^3 - sx - t = 0$ genügt. Die folgende Methode führt dagegen im allgemeinen ohne allzu viel Rechnung zum Ziel: Man bilde eine größere Anzahl von Normen $N(x + y\vartheta)$ mit kleinen x, y, wobei $N(x + y\vartheta)$ auch möglichst kleine Primfaktoren habe. Dann kann man leicht zu einem Quotienten

$$\frac{\Pi(x + y\vartheta)}{\Pi(x' + y'\vartheta)}$$

[3]) J. f. Math. **135** (1909).

mit der Norm 1 gelangen. Dazu muß man aber die wirkliche Primidealzerlegung der $x + y\vartheta$ kennen. Wie schon gesagt, können wir statt einer Einheit ε auch ein $\sigma = \varepsilon\tau^3$, manchmal auch ein $r\sigma$, r rational, gebrauchen [4]).

Wir legen jetzt eine kleine Tabelle niedriger Normen im obigen Körper $\mathsf{P}(\vartheta)$ an:

δ	$\lvert N(\delta)\rvert$	Zerfällung von δ
ϑ	56	$\bar{2}^3 \cdot \bar{7}$
$1 - \vartheta$	12	$\bar{\bar{2}} \cdot \bar{3}$
$1 + \vartheta$	100	$\bar{\bar{2}} \cdot \bar{5}^2$
$2 + \vartheta$	150	$\bar{2} \cdot \bar{3} \cdot \bar{5}$
$3 - \vartheta$	100	$\bar{\bar{2}} \cdot \bar{\bar{5}}$
$4 - \vartheta$	180	$\bar{2}^2 \cdot \bar{3}^2 \cdot \bar{5}$
$7 + \vartheta$	700	$\bar{\bar{2}} \cdot \bar{5} \cdot \bar{7}$

Hierbei bedeutet $\bar{p}$ Primidealfaktor 1. Grades, $\bar{\bar{p}}$ Primidealfaktor 2. Grades von p.

Die Primidealzerlegung erhält man aus den $N(\delta)$ hier so: Der Faktor 3 oder 7 von $N(\delta)$ kann zu δ nur den Beitrag $\bar{3}$ oder $\bar{7}$ liefern, da die Zerlegungen $3 = \bar{3} \cdot \bar{\bar{3}}$ und $7 = \bar{7} \cdot \bar{\bar{7}}$ festliegen und beide Zahlen auch nicht in der Gleichungsdiskriminante aufgehen. 2 und 5 zerfallen entsprechend, falls sie nur außerwesentliche Diskriminantenteiler sind, sonst in der Form $2 = \bar{\bar{2}}_0^2 \cdot \bar{2}_1$ und $5 = \bar{\bar{5}}_0^2 \cdot \bar{5}_1$. Nun sind alle Normen $N(x + y\vartheta)$ gerade, und zwar ist $N(x \pm \vartheta)$ immer durch 4 teilbar, wenn x ungerade, für gerades x aber abwechselnd durch 2 und 4 teilbar, woraus man schließen kann, daß der in 2 in erster Potenz aufgehende Primteiler ersten Grades ($\bar{2}$ oder $\bar{2}_1$) in ϑ, $2 \pm \vartheta, \ldots$ aufgeht, während $\bar{\bar{2}}$ oder $\bar{\bar{2}}_0^2$ in $1 \pm \vartheta$, $3 \pm \vartheta, \ldots$ aufgehen muß. Nämlich aus $\delta \equiv 0(\bar{\bar{2}}^2)$ folgt $\delta + 2 \not\equiv 0(\bar{\bar{2}}^2)$, wenn $\bar{2}$ nur in erster Potenz in 2 aufgeht. Ob nun aber $\bar{\bar{2}}$ oder $\bar{\bar{2}}_0^2 \mid 1 - \vartheta$, jedenfalls ist $2 \mid \vartheta(1 - \vartheta)$, also 2 außerwesentlicher Diskriminantenteiler, und daher hier $2 = \bar{\bar{2}} \cdot \bar{\bar{2}}$. Entsprechend schließt man $\bar{5} \mid 4 - \vartheta$, aber $\bar{\bar{5}}$ oder $\bar{\bar{5}}_0^2 \mid 3 - \vartheta$, also $5 \mid (4 - \vartheta)(3 - \vartheta)$ und damit $5 = \bar{5} \cdot \bar{\bar{5}}$.

Damit haben wir zugleich festgestellt, daß $\mathsf{P}(\vartheta)$ wirklich nur die Diskriminante D hat. — Die außerwesentlichen Diskriminantenteiler eignen sich besonders gut als Normenteiler in der Normentabelle, weil sie viel häufiger als Teiler eines $x + y\vartheta$ auftreten und daher ein gegenseitiges Aufheben der Primteiler leichter bewirken.

Aus der Tabelle können wir nun entnehmen, daß

$$\varepsilon = \frac{(1 + \vartheta)(2 + \vartheta)(3 - \vartheta)(4 - \vartheta)(7 + \vartheta)}{5^3 \cdot \vartheta \cdot (1 - \vartheta)^3}$$

eine Einheit ist, die wir durch

$$\sigma = \varepsilon\tau^3 = \vartheta^2 \cdot (1 + \vartheta)(2 + \vartheta)(3 - \vartheta)(4 - \vartheta)(7 + \vartheta)$$

ersetzen dürfen. Es ist dann nach den Moduln

(73) $\vartheta \equiv -4, -21, 25$

$$\sigma \equiv \pm \begin{cases} 16 \cdot 3 \cdot 2 \cdot 3 \cdot 7 \cdot 8 & \varrho^2 \\ 3 \cdot 20 \cdot 19 \cdot 14 \cdot 24 \cdot 25 & \varrho \\ 32 \cdot 26 \cdot 27 \cdot 32 \cdot 22 \cdot 21 & 1 \end{cases}$$

(19) $\vartheta \equiv 2, 6, -8$

$$\sigma \equiv \pm \begin{cases} 4 \cdot 3 \cdot 4 \cdot 9 \cdot 1 \cdot 2 & \varrho^2 \\ 2 \cdot 7 \cdot 8 \cdot 6 \cdot 3 \cdot 2 & \varrho^2 \\ 7 \cdot 7 \cdot 6 \cdot 1 \cdot 8 \cdot 7 & \varrho^2. \end{cases}$$

Also können wir $q = 19$ setzen, wo dann $\sqrt{D} \equiv \pm 1$. Es ist

[4]) Man muß nur vermeiden, daß $\varepsilon = 1$ oder eine dritte Potenz wird, was aber nicht schwierig ist, da diese im allgemeinen größere Koeffizienten haben.

$$\mathfrak{j}_{13}^3 \equiv \frac{69 \pm 1}{2}; \quad \chi = \varrho, \varrho^2.$$

$$\mathfrak{j}_{19}^3 \equiv \frac{153 \pm 1}{2}; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{19}$ selbst in K_{19} Hauptideal.

Zusammenfassend erhalten wir für $D = -4027$: In K_{17} wird $\mathfrak{j}_{29}$, in K_{29} wird $\mathfrak{j}_{13}$, in K_{13} wird $\mathfrak{j}_{19}$, in K_{19} aber auch $\mathfrak{j}_{19}$ Hauptideal.

II. $D = -9748$.

Reduzierte Formen.	Zugehörige Gleichungen.	Diskriminante.	Körper.
$+ (1, 0, 2437)$			
$- (2, 2, 1219)$			
$- (23, \pm 2, 106)$	$F_{23}(x) = x^3 + x - 38 = 0$	$\Delta = 4D$	$K_{23(53)}$
$+ (46, \pm 2, 53)$			
$- (11, \pm 8, 223)$	$F_{11}(x) = x^3 - 215x - 1214 = 0$	$\Delta = 4D$	$K_{11(22)}$
$+ (22, \pm 14, 113)$			
$+ (41, \pm 16, 61)$	$F_{41}(x) = x^3 - x^2 - 3x - 37 = 0$	$\Delta = 4D$	K_{41}
$- (43, \pm 20, 59)$			
$+ (29, \pm 24, 89)$	$F_{29}(x) = x^3 + 10x - 36 = 0$	$\Delta = 4D$	K_{29}.
$- (47, \pm 34, 58)$			

Idealkuben $\mathfrak{j}^3 = \alpha$:

$$\mathfrak{j}_{53}^3 = 373 + \sqrt{D}, \quad \mathfrak{j}_{22}^3 = 30 + \sqrt{D}, \quad \mathfrak{j}_{41}^3 = 173 + 2\sqrt{D}, \quad \mathfrak{j}_{29}^3 = 121 + \sqrt{D}.$$

Mit $\pm$ haben wir oben das Haupt- und Nebengeschlecht signiert. Als Kapitulanten in den kubischen Klassenkörpern kommen nur die Klassen des Hauptgeschlechts in Frage, während für den Primidealzerfall jedem Paar zueinander inverser Klassen des Hauptgeschlechts noch ein solches aus dem Nebengeschlecht angegliedert ist, wie oben aus den zugehörigen Gleichungen ersichtlich. — Die Gleichungsdiskriminante ist hier jedesmal $4D$; da aber schon D durch 4 teilbar ist, haben die vier Körper nur die Diskriminante D, und es zerfällt immer $2 = \bar{2}_0^2 \cdot \bar{2}_1$. Und zwar schließt man hier bei den ersten beiden Körpern K_{53} und K_{22} entsprechend wie bei K_{19} von $D = -4027$, daß $\bar{2}_1 \mid 2n \pm \vartheta$; $\bar{2}_0 \mid 2n + 1 \pm \vartheta$. Bei K_{29} dagegen: $\bar{2}_0 \cdot \bar{2}_1 \mid 2n \pm \vartheta$. Da sonst nichts Neues hinzukommt, lassen wir jetzt die Rechnungen folgen.

[53] $\quad F(x) = x^3 + x - 38 = 0.$

δ	$\lvert N(\delta)\rvert$	Zerfällung
$1 - \vartheta$	36	$\bar{2}_0^2 \cdot \bar{3}^2$
$2 + \vartheta$	48	$\bar{2}_1^4 \cdot \bar{3}$
$3 - \vartheta$	8	$\bar{2}_0^3$

Es ist $\varepsilon = \dfrac{2^8 \cdot (1 - \vartheta)}{(2 + \vartheta)^2 (3 - \vartheta)^6}$, das sich durch $\sigma = (1 - \vartheta)(2 + \vartheta)$ ersetzen läßt.

(97) $\quad \vartheta \equiv -7, -9, 16$

$\sigma \equiv \pm 8 \cdot 5, 10 \cdot 7, 15 \cdot 18$	$\langle 2\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \langle 13\rangle = \varrho.$
$\langle\sigma\rangle = \varrho, 1, \varrho^2$	

(619) $\quad \vartheta \equiv \dfrac{35}{2}, -147, -180$

$\langle 2\rangle = \langle 5\rangle = \langle 11\rangle = \varrho.\ \langle 7\rangle = \langle 19\rangle = \langle 37\rangle = \varrho^2.$

$\sigma \equiv \dfrac{33 \cdot 39}{4}, 148 \cdot 145, 181 \cdot 178$	$\langle 3\rangle = \langle 13\rangle = \langle 17\rangle = \langle 29\rangle = 1.$
$\langle\sigma\rangle = \varrho^2, \varrho^2, \varrho^2$	

Wir können $q = 619$ setzen. Dann ist

$$\mathfrak{j}_{22}^3 \equiv 30 \pm 67; \quad \chi = \varrho, \varrho^2.$$
$$\mathfrak{j}_{41}^3 \equiv 173 \pm 2 \cdot 67; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{41}$ in K_{53} Hauptideal.

[22] $F(x) = x^3 - 215x - 1214 = 0.$

δ	$\lvert N(\delta)\rvert$	Zerfällung
$9 + \vartheta$	8	$\bar{2}_0^3$
$10 + \vartheta$	64	$\bar{2}_1^6$

$$\varepsilon = \frac{(9+\vartheta)^4(10+\vartheta)}{2^6}, \quad \sigma = (9+\vartheta)(10+\vartheta).$$

(229) $\vartheta \equiv 3, \quad \frac{2}{3}, \quad \frac{-11}{3}$

$\sigma \equiv 12 \cdot 13, \frac{29 \cdot 32}{9}, \frac{16 \cdot 19}{9}$ $\quad \langle 2\rangle = 1.\ \langle 3\rangle = \varrho.\ \langle 5\rangle = \langle 7\rangle = \varrho^2.$

$\langle\sigma\rangle = \varrho, \quad \varrho^2, \quad 1$

(571) $\vartheta \equiv 83, \quad 133, \quad -216$

$\sigma \equiv 92 \cdot 93, 142 \cdot 143, 207 \cdot 206$ $\quad \langle 2\rangle = \langle 5\rangle = \varrho.\ \langle 3\rangle = \langle 11\rangle = \langle 19\rangle = \varrho^2.$ $\langle 7\rangle = \langle 23\rangle = \langle 31\rangle = 1.$

$\langle\sigma\rangle = \varrho, \quad \varrho, \quad \varrho$

Nach dem zulässigen Modul $q = 571$ gilt dann:

$$\mathfrak{j}_{29}^3 \equiv 121 \pm 124; \quad \chi = \varrho, \varrho^2.$$
$$\mathfrak{j}_{22}^3 \equiv 30 \pm 124; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{22}$ in K_{22} Hauptideal.

[41] $F(x) = x^3 - x^2 - 3x - 37 = 0.$

$$\varepsilon = 4 - \vartheta.$$

(43) $\vartheta \equiv -2, -5, \quad 8$ $\qquad$ (193) $\vartheta = -\frac{2}{3}, -25, \quad 91$

$\varepsilon \equiv \quad 6, \quad 9, -4$ $\qquad$ $\varepsilon \equiv \quad \frac{14}{3}, \quad 29, -87$

$\langle\varepsilon\rangle = \varrho, \quad \varrho^2, \quad 1$ $\qquad$ $\langle\varepsilon\rangle = \quad 1, \quad 1, \quad 1$

$\langle 2\rangle = \langle 5\rangle = \langle 19\rangle = \varrho.$
$\langle 7\rangle = \varrho^2.\ \langle 3\rangle = \langle 29\rangle = 1.$

Nach dem zulässigen Modul $q = 193$ gilt dann:

$$\mathfrak{j}_{22}^3 \equiv 30 \pm 45; \quad \chi = \varrho^2, \varrho.$$
$$\mathfrak{j}_{29}^3 \equiv 121 \pm 45; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{29}$ in K_{41} Hauptideal.

[29] $F(x) = x^3 + 10x - 36 = 0.$

δ	$\lvert N(\delta)\rvert$	Zerfällung
ϑ	36	$\bar{2}_0 \cdot \bar{2}_1 \cdot \bar{3}^2$
$2 - \vartheta$	8	$\bar{2}_0 \cdot \bar{2}_1^2$
$2 + \vartheta$	64	$\bar{2}_0 \cdot \bar{2}_1$
$3 - \vartheta$	21	$\bar{3} \cdot \bar{7}$
$4 + \vartheta$	140	$\bar{2}_0 \cdot \bar{2}_1 \cdot \bar{5} \cdot \bar{7}$
$6 - \vartheta$	240	$\bar{2}_0 \cdot \bar{2}_1^3 \cdot \bar{3} \cdot \bar{5}$

Hier sind $\bar{2}_0$ und $\bar{2}_1$ Teiler aller $2n \pm \vartheta$, also bleibt nur $\vartheta = \bar{2}_0 \cdot \bar{2}_1 \cdot \bar{3}^2$, und daher geht $\bar{2}_0$ in allen $2n \pm \vartheta$ nur in erster Potenz auf.

$$\varepsilon = \frac{(3-\vartheta)(6-\vartheta)(2-\vartheta)^2}{\vartheta\,(2+\vartheta)(4+\vartheta)}.$$

(139) $\vartheta \equiv \quad 5, \quad 8, \quad -13$

$$\varepsilon \equiv \frac{\pm 2\cdot 1\cdot 3^2}{5\cdot 7\cdot 9}, \frac{5\cdot 2\cdot 6^2}{8\cdot 10\cdot 12}, \frac{16\cdot 19\cdot 15^2}{13\cdot 11\cdot 9}$$

$\langle 2\rangle = \langle 11\rangle = \langle 13\rangle = \langle 19\rangle = \varrho.$
$\langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \varrho^2.$

$\langle\varepsilon\rangle = \quad 1, \quad \varrho^2, \quad \varrho$

(157) $\vartheta \equiv \quad -8, \quad -12, \quad 20$

$$\varepsilon \equiv \frac{\pm 11\cdot 14\cdot 10^2}{8\cdot 6\cdot 4}, \frac{15\cdot 18\cdot 14^2}{12\cdot 10\cdot 8}, \frac{17\cdot 14\cdot 18^2}{20\cdot 22\cdot 24}$$

$\langle 2\rangle = \langle 7\rangle = 1.$
$\langle 3\rangle = \langle 5\rangle = \langle 11\rangle = \langle 17\rangle = \langle 19\rangle = \varrho.$

$\langle\varepsilon\rangle = \quad \varrho^2, \quad \varrho^2, \quad \varrho^2$

Wir können $q = 157$ setzen, es ist dann:

$$\mathfrak{j}_{22}^3 \equiv 30 \pm 65; \quad \chi = \varrho^2, \varrho.$$
$$\mathfrak{j}_{29}^3 \equiv 121 \pm 65; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{29}$ in K_{29} Hauptideal.

Gesamtresultat für $D = -9748$: In K_{23} wird $\mathfrak{j}_{41}$, in K_{41} wird $\mathfrak{j}_{29}$, in K_{29} wird $\mathfrak{j}_{29}$ selbst und in K_{22} auch $\mathfrak{j}_{22}$ selbst Hauptideal.

III. $D = -3299$.

	Reduzierte Formen.	Zugehörige Gleichungen.	Diskriminante.	Körper.
	$(1, 1, 825)$			
$A^{\pm 3}$	$(27, \pm 7, 31)$			
$C^{\pm 1}$	$(11, \pm 1, 75)$	$F_{11}(x) = x^3 + 2x - 11 = 0$	$\Delta = D$	K_{11}
$(A^3C)^{\pm 1}$	$(15, \pm 11, 57)$			
$(A^3C^{-1})^{\pm 1}$	$(23, \pm 17, 39)$			
$A^{\pm 1}$	$(3, \pm 1, 275)$			
$A^{\pm 2}$	$(9, \pm 7, 93)$	$F_3(x) = x^3 - 16x - 27 = 0$	$\Delta = D$	K_3
$A^{\pm 4}$	$(17, \pm 13, 51)$			
	$(5, \pm 1, 165)$			
	$(25, \pm 1, 33)$	$F_{13}(x) = x^3 - 13x - 112 = 0$	$\Delta = 100D$	K_{13}
	$(13, \pm 9, 65)$			
	$(15, \pm 1, 55)$			
	$(19, \pm 11, 45)$	$F_{19}(x) = x^3 - 19x - 94 = 0$	$\Delta = 64D$	K_{19}.
	$(29, \pm 23, 33)$			

Idealkuben $\mathfrak{j}^3 = \alpha$:

$$\mathfrak{j}_{11}^3 = \frac{45 + \sqrt{D}}{2}, \quad \mathfrak{j}_{23}^3 = \frac{213 + \sqrt{D}}{2}, \quad \mathfrak{j}_{15}^3 = \frac{101 + \sqrt{D}}{2}, \quad \mathfrak{j}_{27}^3 = \frac{128 + \sqrt{D}}{2}.$$

Die Klassengruppe ist hier eine Gruppe $\{A, C\}$, deren Erzeugende A und C die Ordnungen 9 und 3 haben. Unter den vier Untergruppen vom Index 3 ist die Gruppe $\{A^3, C\}$ als einzige nichtzyklische ausgezeichnet und damit der Körper K_{11} unter den vier kubischen Klassenkörpern. Zugleich besteht $\{A^3, C\}$ aus den Elementen der Ordnung 3, also denjenigen, die zur Kapitulation in den kubischen Körpern in Betracht kommen. Unter den vier Untergruppen der Ordnung 3 ist wieder die Gruppe $\{A^3\}$ ausgezeichnet, da ihre Faktorgruppe als einzige nicht zyklisch ist. Dies ist hier aber gerade nicht die Untergruppe, die in K_{11} in die Hauptklasse übergeht, wie wir gleich sehen werden.

[11] $F(x) = x^3 + 2x - 11 = 0.$

$$\varepsilon = 2 - \vartheta.$$

(31) $\vartheta \equiv 5, 6, -11$ (313) $\vartheta \equiv 19, 57, -76$ $\langle 2\rangle = \langle 11\rangle = \langle 13\rangle = \langle 17\rangle = \varrho.$
$\varepsilon \equiv -3, -4, 13$ $\varepsilon \equiv -17, -55, 78$ $\langle 3\rangle = \langle 29\rangle = \varrho^2.$
$\langle\varepsilon\rangle = \varrho, 1, \varrho^2$ $\langle\varepsilon\rangle = \varrho, \varrho, \varrho$ $\langle 5\rangle = \langle 7\rangle = \langle 19\rangle = 1.$

Nach dem zulässigen Modul $q = 313$ gilt dann:

$$\mathfrak{j}_{27}^2 \equiv 128 \pm 12; \quad \chi = \varrho^2, \varrho.$$
$$\mathfrak{j}_{23}^3 \equiv -50 \pm 6; \quad \chi = 1.$$

Es wird also $\mathfrak{j}_{23}$ Hauptideal in K_{11}, nicht $\mathfrak{j}_{27}$.

[3] $F(x) = x^3 - 16x - 27 = 0.$

δ	$\lvert N(\delta)\rvert$	Zerfällung
ϑ	27	$\bar{3}_1^3$
$\vartheta - 4$	27	$\bar{3}_2^3$
$\vartheta + 4$	27	$\bar{3}_3^3$
$\vartheta + 2$	3	$\bar{3}_2$

Also $\varepsilon = \dfrac{\vartheta - 4}{(\vartheta + 2)^3}$; $\quad \sigma = \vartheta - 4.$

(9) $\vartheta \equiv 0, 4, -4$ (277) $\vartheta \equiv 14, 47, -61$
$\sigma \equiv -4, 0, 1$ $\sigma \equiv 10, 43, -65$
$\langle\varepsilon\rangle = \varrho^2, \varrho, 1$ $\langle\sigma\rangle = \varrho^2, \varrho^2, \varrho^2$

$\langle 2\rangle = \langle 13\rangle = 1$; $\langle 3\rangle = \varrho$;
$\langle 5\rangle = \langle 7\rangle = \varrho^2.$

Wir können $q = 277$ setzen; es ist dann

$$\mathfrak{j}_{11}^3 = \frac{45 + \sqrt{D}}{2} \equiv 25, \quad 20; \quad \chi = \varrho, \varrho^2.$$
$$\mathfrak{j}_{23}^3 = \frac{213 + \sqrt{D}}{2} \equiv -168, 104; \quad \chi = 1.$$

Also wird in K_3 wieder $\mathfrak{j}_{23}$ Hauptideal.

[13] $F(x) = x^3 - 13x - 112 = 0.$

2 und 5 sind nur außerwesentliche Diskriminantenteiler, was man ebenso wie bei $F(x) = x^3 + 43x + 56$ erschließen kann. Es ist $N(1 + \delta) = N(17 - 3\vartheta) = 100$. Wegen $(17 - 3\vartheta) + 3(1 + \vartheta) = 20$ gehen in beiden Zahlen dieselben Faktoren von 2 und 5 auf, und da die Norm beide Male nur $= 2^2 \cdot 5^2$, auch in derselben Potenz. Es ist also

$$\varepsilon = \frac{17 - 3\vartheta}{1 + \vartheta}.$$

(13) $\vartheta \equiv 2, 5, 6$ (31) $\vartheta \equiv 1, 3, -4$
$\varepsilon \equiv 8, 9, -2$ $\varepsilon \equiv 7, 2, \frac{2}{3}$
$\langle\varepsilon\rangle = 1, \varrho^2, \varrho$ $\langle\varepsilon\rangle = \varrho, 1, \varrho^2$

(1201) $\vartheta \equiv -17, -410, 427$
$\varepsilon \equiv -\frac{17}{4}, -\frac{103}{2}, 345$
$\langle\varepsilon\rangle = \varrho^2, \varrho, 1$

$\langle 2\rangle = \langle 3\rangle = \langle 11\rangle = \langle 17\rangle = \varrho.$ $\langle 5\rangle = \langle 103\rangle = \varrho^2.$
$\langle 7\rangle = \langle 13\rangle = \langle 19\rangle = \langle 23\rangle = 1.$

Wir haben in diesem Falle gerade nur 3 Moduln r gefunden, für die $\langle\varepsilon\rangle = 1, \varrho, \varrho^2$ ausfällt. Dann gilt mod r für das kapitulierende $\mathfrak{j}_0$ wegen $\mathfrak{j}_0^3 = \alpha_0 = \varepsilon^{s-1}\ \gamma^{3s}$ bestimmt auch nur $\langle\alpha_0\rangle = \varrho, \varrho, \varrho$. Für $\langle\alpha\rangle = 1, 1, 1$ scheidet daher das zugehörige $\mathfrak{j}$ als Kapitulant aus.

Nun ist für

$r = 13$: $\mathfrak{j}_{11}^3 \equiv \dfrac{45 \pm 9}{2}$; $\chi = 1$. $\mathfrak{j}_{11}$ scheidet daher aus.

$r = 31$: $\mathfrak{j}_{15}^3 \equiv \dfrac{101 \pm 7}{2}$; $\chi = 1$. $\mathfrak{j}_{15}$ scheidet daher aus.

$r = 1201$: $\mathfrak{j}_{23}^3 \equiv \dfrac{213 \pm 340}{2} \equiv -324, 537$; $\mathfrak{j}_{23}$ scheidet daher aus.

$\chi = 1$.

Also wird $\mathfrak{j}_{27}$ Hauptideal in K_{13}.

[19] $F(x) = x^3 - 19x - 94 = 0$.

δ	$\lvert N(\delta)\rvert$	Zerfällung
ϑ	94	$\bar{2} \cdot \overline{47}$
$2 + \vartheta$	64	$\bar{2}^6$
$6 - \vartheta$	8	$\bar{2}^3$
$3 + \vartheta$	64	$\bar{2}^3$
$5 - \vartheta$	64	$\bar{2}^3$

Der Körper $\mathsf{P}(\vartheta)$ könnte hier die Diskriminante $D' = D$ oder $= 4D$ haben. Je nachdem zerfällt $2 = \bar{2} \cdot \bar{\bar{2}}$ oder $2 = \bar{2}_0^2 \cdot \bar{2}_1$. Im zweiten Falle hieße es in der Zerfällung der δ statt $\bar{\bar{2}}$ dort $\bar{2}_0^2$. Beide Male aber wäre $8 \mid (5 - \vartheta)(6 - \vartheta)$; also $64D' \mid \Delta$, daher $D' = D$.

Also $\varepsilon = \dfrac{5 - \vartheta}{3 + \vartheta}$.

(19) $\vartheta \equiv -1, -7, 8$ (103) $\vartheta \equiv -19, -25, 44$

$\varepsilon \equiv \pm 3, \quad 3, 8$ $\varepsilon \equiv \pm \frac{3}{2}, \quad 8, 60$

$\langle\varepsilon\rangle = \quad \varrho, \quad \varrho, \varrho$ $\langle\varepsilon\rangle = \quad \varrho^2, \quad 1, \varrho$

Wir können also $q = 19$ setzen. Es gilt dann:

$$\mathfrak{j}_{11}^3 \equiv \frac{45 \pm 11}{2}; \quad \chi = \varrho^2, \varrho.$$

$$\mathfrak{j}_{15}^3 \equiv \frac{101 \pm 11}{2}; \quad \chi = 1.$$

Also wird $\mathfrak{j}_{15}$ Hauptideal in K_{19}.

Für den Körper $\mathsf{P}(\sqrt{-3299})$ mit der Klassengruppe vom Typ (3, 9) besteht also die Kapitulationsordnung:

$$K_{11} \to \mathfrak{j}_{23}; \quad K_3 \to \mathfrak{j}_{23}; \quad K_{13} \to \mathfrak{j}_{27}; \quad K_{19} \to \mathfrak{j}_{15}.$$

Wie schon in der Einleitung gesagt, kann hier in keinem zyklischen Unterkörper 9. Grades des Klassenkörpers eine Klasse der Ordnung 9 kapitulieren, weil in K_{11} nicht $\mathfrak{j}_{27}$, also nicht die dritte Potenzklasse kapituliert. Anders, das sei noch erwähnt, liegt die Sache z. B. für $D = -19427$. Hier hat die Klassengruppe auch den Typus (3, 9); es geht aber in dem kubischen Körper, der der Unterkörper der zyklischen Klassenkörper 9. Grades ist, gerade die dritte Potenzklasse in die Hauptklasse über. Das sagt aber noch nichts darüber, ob in den zyklischen Klassenkörpern 9. Grades hier eine Klasse der Ordnung 9 kapituliert — wie schon das Artin-Furtwänglersche Beispiel $\mathsf{P}\sqrt{(-65)}$ für die entsprechende Zweiergruppe lehrt.

[1] Um ein passendes ϑ zu bestimmen, das einer Gleichung $x^3 - sx - t = 0$ mit der Diskriminante $\Delta = m^2 D$ genügt, hat man nach Lösungen der Diophantischen Gleichung $4s^3 - 27t^2 = m^2 D$ zu suchen. m ist dabei die Transformationsdeterminante einer Körperbasis in die Basis $[1, \vartheta, \vartheta^2]$. Zuerst wird man es im Falle $D \equiv \pm 4$ (9) mit $m = 1$, dann $m = 8$, 10, ... versuchen, also in den Fällen $D = -4027, -3299$, wo wir durch $m = 1$ schon 3 bzw. 2 Gleichungen mit der Diskriminante D gewinnen konnten. Zu beachten ist, daß s mod 9 fest-

liegt (bei festem m), daß man daher nur mit weit auseinanderliegenden s zu rechnen hat, wenn man außerdem noch Kongruenzausscheidungen mod 5, ... vornimmt. Bei $D = -9748$ haben wir alle Gleichungen durch $m = 2$ erhalten. In diesem Falle können wir auch sofort entscheiden, daß D, nicht etwa $4D$, die Körperdiskriminante ist, weil eine kubische Diskriminante nicht durch 16 teilbar sein kann. Für $D = -4027$ muß man dagegen bei der gewonnenen Gleichung $F_{19} = 0$ mit $\Delta = 100D$ noch nachprüfen, daß 2 und 5 nicht in der Körperdiskriminante aufgehen; denn beide Primzahlen kommen gerade als Führer für einen kubischen Ringklassenkörper über $\mathsf{P}(\sqrt{-4027})$ in Betracht. Entweder sucht man nun ein $\vartheta_1 = \frac{a_0 + a_1\vartheta + a_2\vartheta^2}{2}$ und ein $\vartheta_2 = \frac{c_0 + c_1\vartheta + c_2\vartheta^2}{5}$, oder man gewinnt das Resultat aus Primidealzerlegungen im kubischen Körper (vgl. die Normentabelle für F_{19} auf S. 24).

Nun hat man noch darauf zu achten, daß man wirklich für vier verschiedene kubische Körper über $\mathsf{P}(\sqrt{D})$ zugehörige Gleichungen bekommt, die sich also durch verschiedenen Kongruenzzerfall auszeichnen müssen. Dafür gibt es verschiedene Methoden. Z. B. sind F_{13} und F_{29} bei $D = -3299$ dadurch gewonnen, daß der Koeffizient $s \equiv 0 \bmod 13, 19$ gewählt wurde und s dann als kubischer Rest. Es gibt auch eine allgemeine Methode, wenn man erst einmal Gleichungen für zwei Körper hat, aus diesen für die anderen beiden (durch die zwei Körper schon bestimmten) kubischen Körper zugehörige Gleichungen herzuleiten. Seien:

$$F_1(x) = x^3 - s_1x - t_1 = 0, \quad F_2(x) = x^3 - s_2x - t_2 = 0$$

zwei durch Tschirnhausen-Transformation nicht ineinander überführbare kubische Gleichungen mit den Wurzeln $\alpha_1, \alpha_1', \alpha_1''$ und $\alpha_2, \alpha_2', \alpha_2''$ und den Diskriminanten Δ und Δq^2 (q rational), so erzeugt $\alpha_1\alpha_2$ den Körper $\mathsf{P}(\alpha_1, \alpha_2)$ vom Grade 9 (außer wenn $s_1 = s_2 = 0$, was wir hier ausschließen wollen) und dann

$$\alpha_3 = \alpha_1\alpha_2 + \alpha_1'\alpha_2' + \alpha_1''\alpha_2'', \quad \alpha_4 = \alpha_1\alpha_2 + \alpha_1'\alpha_2'' + \alpha_1''\alpha_2'$$

die beiden komplementären kubischen Unterkörper von $\mathsf{P}(\alpha_1, \alpha_2)$. Stellt man

$$\alpha_\nu = \sigma_\nu + \tau_\nu, \quad \alpha_\nu' = \varrho\sigma_\nu + \varrho^2\tau_\nu, \quad \alpha_\nu'' = \varrho^2\sigma_\nu + \varrho\tau_\nu \qquad (\nu = 1, \ldots, 4)$$

als Kubikwurzeln nach der Cardanischen Formel dar, so wird dann

$$\alpha_3 = 3\sigma_1\tau_2 + 3\sigma_2\tau_1 = 3\sqrt[3]{\frac{1}{4}t_1t_2 + \frac{1}{4\cdot 27}\Delta q + \frac{1}{4}(t_2 - t_1q)\sqrt{\frac{-\Delta}{27}}} + 3\sqrt[3]{\ldots}$$

und

$$\alpha_4 = 3\sigma_1\tau_1 + 3\sigma_2\tau_2 = 3\sqrt[3]{\frac{1}{4}t_1t_2 - \frac{1}{4\cdot 27}\Delta q + \frac{1}{4}(t_2 + t_1q)\sqrt{\frac{-\Delta}{27}}} + 3\sqrt[3]{\ldots}\,.$$

Die Gleichungen für α_3 und α_4 lauten dann:

$$F_3(x) = x^3 - 3s_1s_2x - \frac{27t_1t_2 + \Delta q}{2} = 0\,,$$

$$F_4(x) = x^3 - 3s_1s_2x - \frac{27t_1t_2 - \Delta q}{2} = 0\,.$$

Die Diskriminanten der Gleichungen sind: $\Delta_3 = \left(27 \cdot \frac{t_2 - t_1q}{2}\right)^2 \cdot \Delta$ und $\Delta_4 = \left(27 \cdot \frac{t_2 + t_1q}{2}\right)^2 \cdot \Delta$.

Der hier bei der Diskriminante auftretende Faktor 27^2 läßt sich in der Regel noch dadurch herausheben, daß man die gefundene Wurzel $\vartheta = \alpha_3$ oder $\vartheta = \alpha_4$ durch $\frac{\vartheta}{3}$ oder $\frac{\vartheta \pm 1}{3}$ ersetzt. Eine der drei Zahlen ϑ, $\vartheta \pm 1$ ist nämlich immer durch 3 teilbar, außer wenn $\Delta \not\equiv 0(3)$, gleichzeitig aber $9|q \not\equiv 0(27)$ — wobei F_1 und F_2 so numeriert seien, daß q nicht 3 im Nenner hat.

(Man beachte, daß $\Delta \not\equiv 0$ (3), $3|q \not\equiv 0$ (9) bei trinomischen Gleichungen gar nicht vorkommt; dann folgt aus $\Delta = 4s_1^3 - 27t_1^2$ und $s_2 \equiv rs_1$ (9) mit $\frac{r^3}{9} \equiv \pm 1$ (27), daß $3|\alpha_3 + \Delta q, \alpha_4 - \Delta q$.)

[2] Dann ist die Fundamentaleinheit oder irgendeine Einheit von $\mathsf{P}(\vartheta)$, die nicht dritte Potenz ist, entweder selbst Grundeinheit in $K_0(\vartheta)$ oder $(S-1)$-te Potenz der Grundeinheit, und beides könnten wir gebrauchen. Bei beliebigen kubischen Körpern kommen auch beide Möglichkeiten vor. Ist aber, wie hier, D Fundamentaldiskriminante, d. h. $K_0(\vartheta)$ absoluter Klassenkörper über K_0, so tritt stets der erste Fall ein (vgl. A. Scholz, Monatsh. f. Math. u. Phys. 40 (1933)). Wir wollen aber von dieser auf einer ziemlich komplizierten Überlegung beruhenden Tatsache keinen Gebrauch machen, obwohl dadurch manchmal eine Rechnung erspart werden könnte.

[3] Die Dichten berechnet man in der folgenden Weise: Seien $\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4$ die Erzeugenden der vier kubischen Körper und $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ die vier Kuben der für die Kapitulation in Betracht kommenden Ideale in K_0. Es sei zuerst gefragt: Für welche in K_0 zerfallenden Primzahlen p der Form $3n+1$ sind $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ kubische Reste? Antwort: α_ν für die in $K_0(\varrho, \sqrt[3]{\alpha_\nu})$ voll zerfallenden p; $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ für die in $K_0(\varrho, \sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2})$ voll zerfallenden; Relativdichten: 1/3 und 1/9. Zweitens ist aber auch die Relativdichte der in $K_0(\varrho, \vartheta_\nu)$ voll zerfallenden p gerade 1/3, und 1/9 für die in $K_0(\varrho, \vartheta_1, \vartheta_2)$ zerfallenden. Da nun kein ϑ_ν in $K_0(\varrho, \sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2})$ liegt, ist $K_0(\varrho, \sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2}, \vartheta_1, \vartheta_2)/K_0(\varrho)$ vom Grade 81, und die Dichten für die verschiedenen Eigenschaften sind „voneinander unabhängig", d. h. kombinieren sich multiplikativ. (Über $K' = K_0(\varrho)$ besteht zwischen $K'(\sqrt[3]{\alpha_1}, \sqrt[3]{\alpha_2})$ und $K'(\vartheta_1, \vartheta_2)$ eine Reziprozität, aus der sich nach Mitberücksichtigung von $K'(\sqrt[3]{\eta})$, wo η Fundamentaleinheit von $\mathsf{P}(\sqrt{-3D})$, das Resultat von Scholz aus J. f. M. 166, S. 201 ablesen läßt.)

2. Die Gruppe des zweiten Klassenkörpers.

Der Zweck dieses und des nächsten Kapitels ist es, zu zeigen, in welchem Umfang man von dem Hauptidealwerden in den Unterkörpern des Klassenkörpers auf die Struktur des zweiten Klassenkörpers und sogar des ganzen Klassenkörpertums schließen kann. In diesem Kapitel werden zunächst die gruppentheoretisch möglichen Relativgruppen der zweiten Klassenkörper für Zahlkörper mit nichtzyklischer Klassengruppe der Ordnung 9 aufgestellt. Dabei ist die Untersuchung nur insofern auf imaginär-quadratische Zahlkörper zugeschnitten, als vorausgesetzt wird, daß in jedem zyklischen Unterkörper des Klassenkörpers genau eine zyklische Untergruppe der Klassengruppe kapituliert. Im zweiten Teil des Kapitels wird die Relativgruppe des zweiten Klassenkörpers von $\mathsf{P}(\sqrt{-3299})$ ebenfalls aus der Kapitulation bestimmt.

I.

Die Klassengruppe des Grundkörpers habe die Erzeugenden S_1 und S_2, beide von der Ordnung 3. Der Klassenkörper besitzt dann vier kubische Teilklassenkörper K_1, K_2, K_3, K_4, welche zu den aus $S_1, S_2, S_3 = S_1S_2, S_4 = S_1S_2^2$ erzeugten Untergruppen gehören. In diesen Körpern mögen die Klassen $S_{i_1}, S_{i_2}, S_{i_3}, S_{i_4}$ kapitulieren. Wir sagen dann, die Kapitulation sei vom Typus $[i_1, i_2, i_3, i_4]$. Im allgemeinen ist dies keine Permutation der i, sondern es kann in mehreren Körpern dieselbe Klasse kapitulieren, so daß dann einige Klassen in den kubischen Körpern gar nicht zur Kapitulation kommen. Es gibt daher zunächst 256 Kapitulationstypen. Da aber die Numerierung der K_α oder der

Untergruppen $\{S_a\}$ belanglos ist [5]), kommen dabei, wie sich abzählen läßt, nur 19 verschiedene Typen vor.

Wir untersuchen jetzt die zweistufig metabelsche Relativgruppe $\mathfrak{G}$ des zweiten Klassenkörpers [6]) bei vorgegebenem Kapitulationstypus. Die Kommutatorgruppe $\mathfrak{A}$ von $\mathfrak{G}$, zu welcher der erste Klassenkörper gehört, wird durch den Kommutator $A = S_2^{-1}S_1^{-1}S_2S_1$ symbolisch erzeugt, d. h. es lassen sich alle Elemente von $\mathfrak{A}$ als symbolische Potenzen $A^{F(S_1, S_2)}$ darstellen, wo $F(S_1, S_2)$ ein Polynom in S_1, S_2 ist und $A^S = S^{-1}AS$ bedeutet [7]). Der Idealmodul $\mathfrak{M}$ aller Polynome H, für welche A^H das Einheitselement E ist, heißt die symbolische Ordnung von A [8]). Durch die Gleichungen

$$(1) \qquad S_1^3 = A^{F_1(S_1, S_2)}, \qquad S_2^3 = A^{F_2(S_1, S_2)}$$

und die Ordnung $\mathfrak{M}$ ist $\mathfrak{G}$ bestimmt.

Setzen wir

$$(2) \qquad S_1 - 1 = X, \quad S_2 - 1 = Y,$$

$$(3) \qquad 1 + S_1 + S_1^2 = f_1, \quad 1 + S_2 + S_2^2 = f_2,$$
$$\text{und } 1 + S_1S_2 + S_1^2S_2^2 = f_3, \quad 1 + S_1S_2^2 + S_1^2S_2 = f_4,$$

so bestehen notwendig die Relationen

$$(4) \qquad F_1X \equiv F_2Y \equiv 0(\mathfrak{M}),$$

$$(5) \qquad F_1Y = -f_1(\mathfrak{M}), \quad F_2X \equiv f_2(\mathfrak{M}).$$

Analoges gilt für die Indizes 3 und 4 bei $S_3^3 = A^{F_3}$, $S_4^3 = A^{F_4}$.

Umgekehrt ist das Bestehen dieser Relationen hinreichend [9]) für die Existenz der Gruppe $\mathfrak{G}$.

Für die in unseren Rechnungen vorkommenden Polynomideale führen wir folgende Bezeichnungen ein:

$$\begin{aligned}
\mathfrak{L} &= (3, X, Y)\\
\mathfrak{L}_2 &= (3, X^2, XY, Y^2)\\
\mathfrak{L}_3 &= (9, 3X, XY, 3Y)\\
\mathfrak{L}_\alpha &= (3^{\left[\frac{\alpha+1}{2}\right]}, X^\alpha, XY, Y^\alpha)\\
\mathfrak{R}_{\alpha\beta} &= (X^\alpha, XY, Y^\beta, f_3)\\
\mathfrak{T}_{\alpha\beta} &= (X^\alpha, XY, Y^\beta, f_3 \pm X^{\alpha-1}, f_3 \pm Y^{\beta-1}) \qquad (6)\\
\mathfrak{V}_{\alpha\beta} &= (X^\alpha, Y^\beta, f_3, XY \pm X^{\alpha-1}, XY \pm Y^{\beta-1})\\
\mathfrak{X}_\alpha &= (X^\alpha, XY, Y^2, f_1)\\
\mathfrak{Z} &= (3, XY, X^2 - Y^2)\\
\mathfrak{Z}' &= (X^3, XY, Y^3, 3 + X^2, 3 - Y^2)\\
\mathfrak{Z}_\alpha &= (X^\alpha, XY, Y^3, f_1 - Y^2, f_1 \pm X^{\alpha-1})\\
\mathfrak{Z}'_\alpha &= (X^\alpha, XY, Y^3, f_1, X^{\alpha-1} \pm Y^2).
\end{aligned}$$

Dabei bezeichnen $\mathfrak{T}_{\alpha\beta}$ und $\mathfrak{V}_{\alpha\beta}$ je 4, dagegen $\mathfrak{Z}_\alpha$ und $\mathfrak{Z}'_\alpha$ je 2 verschiedene Moduln, je nach den offen gelassenen Vorzeichen. — Die als Ordnung von A in Betracht kommen-

[5]) Im allgemeinen Falle einer Gruppe vom Typ (l, l) kann man mit $\{S_1\}$, $\{S_2\}$, $\{S_1S_2\}$ drei beliebige zyklische Untergruppen bezeichnen, wodurch S_1 und S_2 bis auf eine gemeinsame Potenz bestimmt sind und damit die übrigen $\{S_1S_2^\lambda\}$ festliegen.

[6]) Unter Klassenkörper wird stets der absolute vollständige l-Klassenkörper für $l = 3$ verstanden. Siehe Hasse, Bericht II, S. 174.

[7]) Siehe Furtwängler, Hamb. Sem. Abh. **7**, S. 18.

[8]) Siehe Scholz, Math. Zeitschr. **30**, S. 336.

[9]) Siehe Schreier, Hamb. Sem. Abh. **4**, S. 325.

den Ideale gruppieren sich folgendermaßen: $\mathfrak{R}_{\alpha\beta}$ geht für $\beta = 2$ in $\mathfrak{X}_\alpha$ über und dies für $\alpha = 2$ in $\mathfrak{L}_2$. $\mathfrak{T}_{\alpha\beta}$ und $\mathfrak{V}_{\alpha\beta}$ sind als Varianten von $\mathfrak{R}_{\alpha\beta}$ zu betrachten, und es gilt

$$\begin{array}{c} \mathfrak{Z}_\alpha \xrightarrow[\alpha=3]{} \mathfrak{Z} \\ \mathfrak{T}_{\alpha\beta} \xrightarrow[\beta=3]{} \mathfrak{Z}'_\alpha \xrightarrow[\alpha=3]{} \mathfrak{Z}' \end{array}$$

An sich käme auch $\mathfrak{R}_{11} = \mathfrak{L}$ als Ordnung in Betracht. Nach der in Kap. 1, Anm. [2] zitierten Abhandlung müssen aber α und β bei $\mathfrak{R}_{\alpha\beta}$ gerade, bei $\mathfrak{T}_{\alpha\beta}$ und $\mathfrak{V}_{\alpha\beta}$ ungerade sein. Für $\mathfrak{M} = \mathfrak{L}$ ergibt sich der Widerspruch sogar ohne Heranziehung der Einheiten lediglich aus der Galoisgruppe: Es müßte in diesem Fall der zweite Klassenkörper von $\mathsf{P}(\sqrt{D})$ eine absolute Galoisgruppe der Ordnung 54 haben, deren Kommutatorgruppe unsere zweistufige Gruppe der Ordnung 27 ist; eine solche Gruppe gibt es aber nicht.

Weiter bezeichnen wir die Klasse S_a des Grundkörpers und die ihr nach dem Artinschen Reziprozitätsgesetz zugeordnete Substitution mit dem gleichen Symbol. Daß S_{i_a} im Körper K_a zur Hauptklasse wird, läßt sich dann nach Artin [10]) auf eine gruppentheoretische Relation zurückführen. Betrachten wir nämlich den Klassenkörper über K_a als Unterkörper des zweiten Klassenkörpers über K_0, so entsprechen der Hauptklasse von K_a und nur dieser die Elemente der Kommutatorgruppe von $\{S_a, \mathfrak{A}\}$, welche wir symbolisch durch $\{A^{S_a-1}\}$ darstellen können. Wir müssen also zunächst feststellen, welches die den Klassen von K_0 in K_a zugeordneten Substitutionen, die sogenannten Verlagerungen [11]) sind.

Für $i_a \not\equiv a$ entspricht der Klasse S_{i_a} in K_a die Substitution $A^{F_{i_a}}$. Soll S_{i_a} in K_a zur Hauptklasse werden, so muß daher gelten

$$F_{i_a} \equiv 0(\mathfrak{M}, S_a - 1). \tag{7}$$

Für $i_a = a$ entspricht S_{i_a} die Substitution $S_{i_a}^{f_c}$ mit $c \not\equiv a$. Im Falle der Kapitulation muß also gelten:

$$S_a^{f_c} < \{A^{S_a-1}\}. \tag{8}$$

Die Kommutatorgruppe $\{A^{S_a-1}\}$ ist für $a = 1, 2$ durch $\{A^X\}$, $\{A^Y\}$ gegeben; für $a = 3$ durch $\{A^{X+Y+XY}\}$, für $a = 4$ durch $\{A^{S_1S_2^{-1}-1}\} = \{A^{S_1-S_2}\} = \{A^{X-Y}\}$.

Da in (8) $c \not\equiv a$, aber sonst beliebig gewählt werden kann, kommen wir mit f_1 und f_2 aus; es ist z. B.

$$\begin{aligned} S_2^{f_1} &\equiv S_2^{3+3X+X^2} \equiv A^{F_2+3+X} \pmod{A^Y} \\ (S_1S_2)^{f_1} &\equiv (S_1S_2)^{3+3X+X^2} \equiv A^{F_2+3+X} \pmod{A^{X+Y+XY}} \\ S_1^{f_2} &\equiv S_1^{3+3Y+Y^2} \equiv A^{F_1-3-Y} \pmod{A^X} \\ (S_1S_2^2)^{f_2} &\equiv (S_1S_2^2)^{3+3Y+Y^2} \equiv A^{F_4-3-Y} \pmod{A^{X-Y}}. \end{aligned} \tag{9}$$

Aus F_1 und F_2 gehen zwar $F_3 = F_1 + F_2 + T_1$ und $F_4 = F_1 + 2F_2 + T_2$ mit festem T_1 und T_2 hervor. Jedoch ergeben T_1 und T_2 so komplizierte Ausdrücke, daß wir uns mit der Feststellung der Kongruenzen

$$\begin{aligned} F_3 &\equiv F_1 + F_2 + X - Y \quad \bmod \mathfrak{L}_2 \\ F_4 &\equiv F_1 - F_2 - X - Y \quad \bmod \mathfrak{L}_2 \end{aligned} \tag{10}$$

begnügen.

Den eigentlichen Resultaten schicken wir noch zwei Bemerkungen voraus:

1. Ist K_0 ein imaginär-quadratischer Körper, so kann nicht $\mathfrak{M} = (1)$ sein, da sonst in jedem der kubischen Teilklassenkörper bereits alle Ideale des Grundkörpers kapitulieren müßten. D. h. aber: Die Klassenzahl des Klassenkörpers ist bestimmt durch 3 teilbar, der zweite Klassenkörper ist zweistufig, der Klassenkörperturm schließt nicht schon mit dem ersten Klassenkörper ab.

[10]) Siehe Artin, Hamb. Sem. Abh. **7**, S. 46.

[11]) Siehe Hasse, Bericht II, S. 170.

2. Die Ordnung $\mathfrak{M} \neq (1)$ ist stets durch das Primideal $\mathfrak{L} = (3, X, Y)$ teilbar, d. h. daß kein Ausdruck $1 + L \equiv 0(\mathfrak{M})$ sein kann, wo $L < \mathfrak{L}$ [12]).

Beweis. Es gibt sicher ein k, so daß $3^k \equiv 0(\mathfrak{M})$. Da S^3 in der Gruppe $\mathfrak{A}$ liegt, ist $S_1^3 - 1 = X^3 + 3X^2 + 3X \equiv 0$ und ebenso $Y^3 + 3X^2 + 3Y \equiv 0(\mathfrak{M})$. Es gibt daher auch eine Zahl m, so daß X^m und $Y^m \equiv 0(\mathfrak{M})$ und jedes $(1 + L)^m \equiv 1(\mathfrak{M})$ ist. Da $\mathfrak{M} \neq (1)$, kann also nicht $1 + L \equiv 0(\mathfrak{M})$ sein. Dieser Sachverhalt gibt uns die Möglichkeit, durch alle Ausdrücke $J \not\equiv 0(\mathfrak{L})$ zu dividieren.

Wir verwenden den Buchstaben J im folgenden immer für Polynome $\not\equiv 0(\mathfrak{L})$, den Buchstaben L für Polynome aus $\mathfrak{L}$ und schreiben außerdem

$$F' \sim F''(\mathfrak{M}),$$

wenn $F'' \equiv F'J(\mathfrak{M})$, speziell $F'' \approx F'$, wenn $J \equiv 1(\mathfrak{L})$. Es ist insbesondere

$$X^3 \sim 3X, \quad Y^3 \sim 3Y(\mathfrak{M}). \tag{11}$$

Wir wenden uns nun dem Ziel dieses Abschnittes zu und beweisen zunächst:

A. *Ist $\mathfrak{M}$ nicht durch $\mathfrak{L}_2$ teilbar, so geht in allen vier kubischen Klassenkörpern dieselbe Klasse, etwa S_1, in die Hauptklasse über; es ist dann $\mathfrak{M} = \mathfrak{L}$ und $S_1^3 = E$, $S_2^3 = A$.*

Beweis. Jedes Polynom L aus $\mathfrak{L}$ läßt sich in der Form $L = aX + bY + L_2$ darstellen, wo $L_2 < \mathfrak{L}_2$ und $a, b = 0, 1, 2$ ist. Soll also $\mathfrak{L}_2 \mid \mathfrak{M}$ nicht gelten, so muß irgendein $L \equiv 0(\mathfrak{M})$ sein, d. h. entweder X oder Y oder $X \pm Y \equiv 0(\mathfrak{L}_2, \mathfrak{M})$. Wir können die Numerierung der S_i so wählen, daß etwa $Y \equiv 0(\mathfrak{L}_2, \mathfrak{M})$ ist, d. h. $Y \equiv 3R_1 + Q_1X^2 + Q_2XY + Q_3Y^2(\mathfrak{M})$ oder nach Division durch $1 - Q_2X - Q_3Y$

$$Y \equiv 3R + QX^2(\mathfrak{M}). \tag{12}$$

Wir unterscheiden nun zwei Fälle:

α) Die Klasse S_2 kapituliere in einem Körper K_a. Wir zeigen, daß in diesem Falle S_2 in sämtlichen K_a kapitulieren muß.

Zufolge (7), (8), (9) muß $F_2 \equiv 0(\mathfrak{L})$ sein, wenn S_2 in einem kubischen Körper kapituliert. Daraus folgt mit Hilfe von (5) und (11), daß $3 \equiv LX + KY^2$ oder $3 \equiv K_1X^2 + K_2XY + K_3Y^2(\mathfrak{M})$, und auf Grund von (12) folgt weiter $3 \equiv 9K_4 + K_5X^2$, also $3 \sim K_5X^2(\mathfrak{M})$. Mit 3 ist aber nach (12) auch $Y \sim K_6X^2(\mathfrak{M})$, so daß mod $\mathfrak{M}$ jedes Element von $\mathfrak{L}$ durch X teilbar ist. Das bedeutet für die Kapitulation, daß in K_1 jede Klasse S_a, für welche $F_a \equiv 0(\mathfrak{L})$ ist, kapitulieren muß. Da aber nur eine Klasse kapitulieren kann und $F_2 \equiv 0(\mathfrak{L})$ ist, muß $F_1, F_3, F_4 \not\equiv 0(\mathfrak{L})$ sein, d. h. $F_1 \sim F_3 \sim F_4 \sim 1(\mathfrak{M})$. Die Klassen S_1, S_3, S_4 können daher auch in anderen Körpern K_a nicht kapitulieren, so daß S_2 allein zur Kapitulation gelangt.

β) S_2 kapituliere nirgends. Da eine Klasse kapitulieren muß, können wir annehmen, es sei dies S_1. Daraus können wir $F_1 \equiv 0(\mathfrak{L})$ schließen und analog wie unter α) ableiten, daß $\mathfrak{L} \equiv 0(X^2)$ mod $\mathfrak{M}$ ist. Dann müssen aber wieder alle Klassen S_a, für welche $F_a \equiv 0(\mathfrak{L})$ ist, in K_1 kapitulieren, woraus folgt, daß in jedem kubischen Körper S_1 und nur S_1 kapituliert.

Damit ist bewiesen, daß für $\mathfrak{M} \not\equiv 0(\mathfrak{L}_2)$ der Kapitulationstyp [1 1 1 1] vorliegt [13]), und daß für jede Klasse S_a, die nirgends kapituliert, $F_a \sim 1(\mathfrak{M})$ gilt. Daraus folgt mit Hilfe der Relationen (4), daß $X \equiv 0(\mathfrak{M})$. Da $\mathfrak{L} < (\mathfrak{M}, X)$, ergibt sich, daß $\mathfrak{L} < \mathfrak{M}$,

---

[12]) Dies gilt auch im allgemeinsten Falle zweistufiger Gruppen von Primzahlpotenzordnung l^m mit $\mathfrak{L} = (l, X, Y)$. Vgl. Scholz, Heidelbg. Ak. Ber. 1933, Nr. 2.

[13]) Dieser Typus kann zwar nach der obigen Bemerkung in Kleindruck (S. 33) nicht vorkommen. Doch wollen wir diese Bemerkung in den folgenden Diskussionen nicht berücksichtigen, die dann auch für andere Grundkörper gelten. Daß dieser Typus dann tatsächlich auftritt, zeigt ein von Scholz angegebener aus kubischen Körpern aufgebauter Körper. Siehe hierzu O. Taussky, J. f. Math. **168**, S. 209.

was mit $\mathfrak{L} \mid \mathfrak{M}$ zusammenbetrachtet zu $\mathfrak{M} = \mathfrak{L}$ führt. Bezeichnen wir die kapitulierende Klasse mit S_1, so folgt: $S_1^3 = E$, $S_2^3 = A^{\pm 1}$.

Der Typus [1 1 1 1] ist also der einzige, wo die Klassengruppe des ersten Klassenkörpers nur die Ordnung 3 hat. Für alle anderen Typen ist sie wegen $\mathfrak{L}_2 > \mathfrak{M}$ mindestens von der Ordnung 27 und nicht mehr zyklisch.

Wir setzen nun im folgenden stets voraus, daß $\mathfrak{M} \equiv 0(\mathfrak{L}_2)$ ist. Wir können dann oft schon durch Betrachtungen mod $\mathfrak{L}_2$ die Beweise führen und bemerken vorweg, daß aus (5) allgemein $f_1 \equiv 0(\mathfrak{M}, Y)$ folgt, also hier $3 + 3X + X^2 \equiv LY(\mathfrak{M})$ wegen $\mathfrak{M} < \mathfrak{L}_2$, d. h.

$$3 \equiv PX^2 + QXY + RY^2(\mathfrak{M}).$$

In der Regel werden wir auf $XY \equiv 0(\mathfrak{M})$ stoßen; dann ist 3 und damit auch jedes $L_2 < \mathfrak{L}_2$ in der Form

$$X^2P(X) + Y^2Q(Y) \tag{13}$$

darstellbar. Wir betrachten jetzt unter B.—H. die weiteren 18 Kapitulationstypen.

B. *Kapituliert die Klasse S_a im Körper K_a, so kann sie unmöglich noch in zwei anderen kubischen Körpern kapitulieren. Damit ist bewiesen, daß die Typen* [1 1 1 2] und [1 2 1 1] unmöglich sind.

Beweis. Die Numerierung sei so gewählt, daß S_3 in K_1, K_2, K_3 kapituliere. Dann muß nach (7) gelten: $F_3 \equiv F'X \equiv F''Y(\mathfrak{M})$, also $F_3 \equiv 0(\mathfrak{L}_2)$. Anderseits folgt aus (8) und (9) die Beziehung $F_3 + X \equiv 0(\mathfrak{L}_2, X + Y)$, welche damit in Widerspruch steht.

C. *Die drei Permutationstypen* [1 2 3 4], [1 3 4 2], [2 3 4 1] sind gruppentheoretisch unmöglich.

Wir beweisen nur die Unmöglichkeit von [1 2 3 4], da die beiden anderen Fälle analog zu behandeln sind.

Schon mod $\mathfrak{L}_2$ müßte zufolge (9) gelten:

$$F_1 \equiv Y + aX, \quad F_2 \equiv -X + bY, \quad F_3 \equiv -X + c(X + Y), \quad F_4 \equiv X + d(X - Y).$$

Aus (10) folgt aber

$$F_3 \equiv F_1 + F_2 + X - Y \equiv aX + bY, \quad F_4 \equiv F_1 - F_2 - X - Y \equiv aX - bY.$$

Aus den beiden Relationen für F_3 ergibt sich $a \equiv b - 1(3)$, für F_4 dagegen $a \equiv b + 1(3)$, was einen Widerspruch ausmacht.

D. *Die beiden Typen* [1 1 2 3] *und* [1 2 1 2] *führen eindeutig auf* $\mathfrak{M} = \mathfrak{L}_2$.

Wir bringen den Beweis wieder nur für einen der beiden Fälle, und zwar für [1 1 2 3], was der Kapitulationstyp von $\mathsf{P}(\sqrt{-4027})$ ist. Wir formen aber das Kapitulationsschema auf [2 3 4 4] um, weil in dieser Anordnung der S_i bald die Relation $XY \equiv 0(\mathfrak{M})$ zum Vorschein kommt. Für das Bestehen dieses Typus ist zunächst notwendig, daß mod $\mathfrak{L}_2$ gilt:

$$F_2 \equiv aX, \quad F_3 \equiv bY, \quad F_4 \equiv c(X + Y) \equiv Y + d(X - Y),$$

was $d \equiv c \equiv -1(3)$ liefert, also $F_4 \equiv -X - Y$. Die Anwendung beider Kongruenzen (10) ergibt einzeln

$$F_1 \equiv -(a + 1)X + (b + 1)Y$$
$$F_1 \equiv aX,$$

also $a \equiv 1$, $b \equiv -1(3)$ und somit:

$$F_1 \equiv X, \; F_2 \equiv X, \; F_3 \equiv -Y, \; F_4 \equiv -X - Y(\mathfrak{L}_2).$$

F_2, F_3, F_4 müssen aber auch mod $\mathfrak{M}$ durch X, Y, $X + Y + XY$ teilbar sein und daher $\sim X$, Y, $X + Y + XY$ wegen der Kongruenzen mod $\mathfrak{L}_2$. Durch Anwendung von (4) nacheinander auf F_2, F_3, F_4 folgt daher $XY \equiv 0(\mathfrak{M})$, $Y(X + Y + XY) \equiv Y^2 \equiv 0(\mathfrak{M})$, $(X - Y)(X + Y) \equiv X^2 \equiv 0(\mathfrak{M})$. Es liegt also auch 3 in $\mathfrak{M}$, und folglich ist $\mathfrak{M} = \mathfrak{L}_2$. Da nun auch F_1 und F_2 festliegen, ist die zweistufige Gruppe bestimmt.

E. *Die vier Typen* [1 1 2 2], [1 2 3 1], [1 2 1 3], [2 3 1 1] *führen bei passender Numerierung der* S_i *auf eine einparametrige Schar von Ordnungen* $\mathfrak{X}_\alpha = (X^\alpha, XY, Y^2, f_1)$ mit $\alpha \geqq 3$. Jedes α läßt zwei Wertepaare F_1, F_2 zu.

Wir führen den Beweis für den Typus [1 1 2 2], den wir durch [2 2 1 1] ersetzen. Wir erhalten dann mod $\mathfrak{L}_2$:

$$F_1 \equiv c(X+Y) \equiv d(X-Y) \equiv 0,\ F_2 \equiv aX \equiv -X+bY, \quad \text{also}$$
$$F_1 \equiv 0,\ F_2 \equiv -X,\ F_3 \equiv F_4 \equiv -Y.$$

Daher kann $\mathfrak{M} = \mathfrak{L}_2$ nicht eintreten, da sonst S_1 auch in K_2 kapitulieren müßte. Wegen $F_2 \sim X$ ist (4) zufolge $XY \equiv 0(\mathfrak{M})$. Außerdem folgt aus (5):

$$-F_1 Y \equiv L_2 Y \equiv KY^3 \equiv 3 + 3X + X^2 = f_1$$

und aus (4):

$$F_4(X-Y) \equiv Y^2 + L_2'(X-Y) \equiv Y^2 + K'X^3 + K''Y^3 \equiv 0(\mathfrak{M}).$$

Es ist also $Y^2 < (\mathfrak{L}_3, \mathfrak{M})$. Da $f_1 < (\mathfrak{L}_3, \mathfrak{M})$ und $3X \sim X^3$, enthält $(\mathfrak{L}_3, \mathfrak{M})$ entweder gleichzeitig 3 und X^2 oder keines von beiden. $(\mathfrak{L}_2, \mathfrak{M}) = (\mathfrak{L}_3, \mathfrak{M})$ kann aber nicht eintreten, weil sonst $(\mathfrak{L}_2, \mathfrak{M}) = (\mathfrak{L}_3, \mathfrak{M}) = (\mathfrak{L}_4, \mathfrak{M}) = \cdots = \mathfrak{M}$ gelten müßte. Es liegen also 3 und X^2 nicht in $\mathfrak{M}$, so daß wir $F_2 \equiv -3 - X + RY^2(\mathfrak{M})$ ansetzen müssen, damit S_2 in K_2 gemäß (8), (9) kapituliert. Wegen $XY \equiv 0(\mathfrak{M})$ läßt sich aber F_1 in der Form (13) darstellen, und das ergibt wegen $F_1 X \equiv 0(\mathfrak{M})$, aber $F_1 \not\equiv 0(\mathfrak{M}, Y)$:

$$F_1 \equiv \pm X^{\alpha-1} + QY^2,$$

wenn α die kleinste Zahl ist, daß $X^\alpha \equiv 0(\mathfrak{M})$, $\alpha \geqq 3$. Durch Anwendung von (5) auf F_1 und F_2 ergibt sich: $-QY^3 \equiv 3 + 3X + X^2$, $-3X - X^2 \equiv 3 + 3Y + Y^2$, also $QY^3 \equiv 3Y + Y^2$ und daraus $Y^2 \equiv 0$ und $f_1 \equiv 0(\mathfrak{M})$. Wegen $F_1 \not\equiv 0(Y)$ ist $X^{\alpha-1} \not\equiv KY(\mathfrak{M})$ und folglich $\mathfrak{M}$ eindeutig bestimmt:

$$\mathfrak{M} = (X^\alpha, XY, Y^2, f_1) \quad \text{und} \quad F_1 = \pm X^{\alpha-1}, \quad F_2 = -3 - X.$$

Ähnlich, nur einfacher wie beim explizit behandelten Typus [1 1 2 2], folgt das analoge Resultat für den Kapitulationstyp [1 2 1 3]. Diesem Typ entspricht der Körper $\mathsf{P}(\sqrt{-9748})$, und seine zweistufige Gruppe lautet, wenn man den Kapitulationstyp auf [2 3 3 4] transformiert:

$$\mathfrak{M} = \mathfrak{X}_\alpha \quad \text{und} \quad F_1 \equiv -Y \pm X^{\alpha-1}, \quad F_2 \equiv -3 - X \mp X^{\alpha-1},$$
$$F_3 \equiv Y, \qquad F_4 \equiv Y \mp X^{\alpha-1}.$$

F. *Den vier Typen* [2 1 1 2], [1 3 2 1], [3 2 1 1] *und* [2 1 1 3] *entspricht eine zweiparametrige Schar von Ordnungen* $\mathfrak{R}_{\alpha\beta} = (X^\alpha, XY, Y^\beta, f_3)$ *mit* $\alpha, \beta \geqq 3$ *und* $f_3 = 1 + S_1 S_2 + S_1^2 S_2^2$; *für* F_1, F_2 *ergeben sich je vier Lösungen.*

Wir beschränken uns auf die Behandlung des schwierigsten Falles [14]) [2 1 1 2], welchen wir auf [3 4 4 3] umformen. Es gilt dann mod $\mathfrak{L}_2$:

$$F_1 \equiv Y, \quad F_2 \equiv -X, \quad F_3 \equiv F_4 \equiv 0.$$

$\mathfrak{M} = \mathfrak{L}_2$ ist wieder ausgeschlossen. Durch Anwendung von (4) auf $F_1 \equiv J_1 Y + QX^2$ und $F_2 \equiv J_2 X + RY^2$ ergibt sich zunächst nur: $XY \sim X^\varkappa \sim Y^\lambda$, $\varkappa, \lambda \geqq 3$. Nun folgt $X^2 Y \sim XY^\lambda \sim X^\varkappa Y^{\lambda-1}$, was $X^2 Y \equiv 0$ liefert, da $X^2 Y$ echter Teiler von $X^\varkappa Y^{\lambda-1}$ ist. Ebenso ist $XY^2 \equiv 0$ und damit $X^{\varkappa+1} \equiv Y^{\lambda+1} \equiv 0$. Da $F_3 \equiv KX, \not\equiv KY$ und $F_3(X+Y) \equiv 0$ ist, kann man F_3 in der Form $\pm X^{\varkappa-1} + \varepsilon XY$, $\varepsilon = 0, 1, 2$, ansetzen; aus $F_3(X+Y) \equiv 0$ folgt dann $X^\varkappa \equiv 0 \equiv XY \equiv Y^\lambda$, aus $F_3 X \equiv f_3$ folgt $f_3 \equiv 0$. Es ist also

$$\mathfrak{M} = \mathfrak{R}_{\varkappa\lambda},\ F_3 \equiv \pm X^{\varkappa-1},\ F_4 \equiv \pm Y^{\lambda-1}.$$

G. *Die Typen* [2 1 4 3] *und* [2 1 3 4]. *Hier ergeben sich je vier Möglichkeiten für die Ordnungen der Gruppe, und zwar* $\mathfrak{L}_2$, $\mathfrak{Z}$; $\mathfrak{R}_{\alpha\beta}$, $\mathfrak{T}_{\alpha\beta}$ *für* [2 1 4 3]; $\mathfrak{X}_\alpha$, $\mathfrak{Z}_\alpha$; $\mathfrak{R}_{\alpha\beta}$, $\mathfrak{V}_{\alpha\beta}$ *für*

[14]) Es ist der Kapitulationstyp des (oben nicht behandelten) Körpers $\mathsf{P}(\sqrt{-3896})$.

[2 1 3 4]. *Die Werte der* F_1, F_2 *ergeben sich im ersten Falle* 1- *bzw.* 9-, 4-, 36-*deutig*; *im zweiten Falle* 2- *bzw.* 18-, 4-, 36-*deutig.*

[2 1 4 3]: mod $\mathfrak{L}_2$ erhalten wir eine dreiwertige Lösung:

A:	$F_1 \equiv -Y$,	$F_2 \equiv X$,	$F_3 \equiv -X+Y$,	$F_4 \equiv X+Y$
B:	Y,	$-X$,	0,	0
C:	0,	0,	$X-Y$,	$-X-Y$.

Für [2 1 4 3] A ergibt (4) mod $\mathfrak{M}$: $XY \equiv 0$, $X^2 - Y^2 \equiv 0$, woraus $X^3 \equiv Y^3 \equiv 0$ folgt. (5) ergibt auf $F_2 \equiv X + KX^2$ angewandt: $X^2 \equiv 3 + 3Y + Y^2$, also $3 \equiv X^2 - Y^2 \equiv 0(\mathfrak{M})$. Es ist also entweder $\mathfrak{M} = \mathfrak{L}_2$ oder $\mathfrak{M} = \mathfrak{Z}$.

Im Falle [2 1 4 3]B, auf welchen sich auch Fall C durch Umnumerierung $S_1, S_2 \longleftrightarrow S_3, S_4$ transformieren läßt, folgt aus (4) wieder $XY \equiv 0$. Sind $\varkappa$, λ die kleinsten Zahlen, für welche $X^\varkappa \sim Y^\lambda$, so ist $X^{\varkappa+1} \equiv Y^{\lambda+1} \equiv 0$. Da $F_3 \equiv 0(\mathfrak{L}_2)$, $\not\equiv KX, KY$, kann man ansetzen: $F_3 \equiv a_1 X^{\varkappa-1} + a_2 Y^{\lambda-1}$, $a_1, a_2 \not\equiv 0(3)$. Es folgt daraus $F_3(X+Y) \equiv a_1 X^\varkappa + a_2 Y^\lambda \equiv 0$, also $f_3 \equiv F_3 X \equiv a_1 X^\varkappa \equiv -a_2 Y^\lambda$. Es ist also entweder $\mathfrak{M} = \mathfrak{R}_{\varkappa\lambda}$ oder $\mathfrak{M} = (X^{\varkappa+1}, XY, Y^{\lambda+1}, f_3 - a_1 X^\varkappa, f_3 + a_2 Y^\lambda)$; $\varkappa, \lambda \geqq 3$.

[2 1 3 4] liefert mod $\mathfrak{L}_2$ die folgenden drei Möglichkeiten:

A:	$F_1 \equiv Y$,	$F_2 \equiv X$,	$F_3 \equiv -X$,	$F_4 \equiv X$
B:	$-Y$,	$-X$,	Y,	Y
C:	0,	0,	$X-Y$,	$-X-Y$.

[2 1 3 4]A läßt sich durch Umnumerierung von S_1 und S_2 auf B transformieren; dort erhalten wir durch Anwendung von (4) und (5) auf F_1: $XY \equiv 0$, $Y^2 \approx f_1$. F_3 können wir dann in der Form

$$F_3 \equiv J_1 Y + J_2 X^{\varkappa-1} \not\equiv FY (\varkappa \geqq 3)$$

ansetzen. Es folgt dann aus

$$F_3(X+Y) \equiv J_1 Y^2 + J_2 X^\varkappa \equiv 0,$$

daß $X^\varkappa \sim Y^2$; $X^{\varkappa+1} \equiv Y^3 \equiv 0$. Es wird entweder $\mathfrak{M} = \mathfrak{X}_\varkappa$ oder $\mathfrak{M} = \mathfrak{Z}_{\varkappa+1}$.

[2 1 3 4]C formen wir auf [1 2 4 3] mit

$$F_1 \equiv Y, \quad F_2 \equiv -X, \quad F_3 \equiv F_4 \equiv 0(\mathfrak{L}_2)$$

um. Wir können hier nicht $XY \equiv 0(\mathfrak{M})$ schließen, sondern es folgt wie unter F erst nur $XY \sim X^\varkappa \sim Y^\lambda (\varkappa, \lambda \geqq 3)$; $X^2 Y \equiv XY^2 \equiv X^{\varkappa+1} \equiv Y^{\lambda+1} \equiv 0$. (5) ergibt dann, etwa auf $F_2 \equiv -3 - X(\mathfrak{M}, Y^2)$ angewandt

$$H = 3 + 3X + X^2 + 3Y + Y^2 \equiv 0,$$

was wegen $f_3 - H \approx -XY$ und $\mathfrak{L}XY \equiv 0$ zu $f_3 \equiv -XY$ führt. Wegen $F_1 \equiv Y + 3 \equiv -2Y + Y^2(\mathfrak{M}, X)$ muß

$$F_1 \equiv -2Y + Y^2 + a_1 X^{\varkappa-1} + c_1 XY \quad (a_1 = \pm 1;\ c_1 = 0, 1, 2)$$

ausfallen, damit $F_1 X \equiv 0(\mathfrak{M})$, aber $F_1 \not\equiv 0(\mathfrak{M}, Y)$. Entsprechend

$$F_2 \equiv 2X + X^2 + a_2 Y^{\lambda-1} + c_2 XY.$$

Es ist $\mathfrak{M} = \mathfrak{R}_{\varkappa\lambda}$ oder $= (X^{\varkappa+1}, Y^{\lambda+1}, f_3 + XY, XY + a_1 X^\varkappa, XY - a_2 Y^\lambda)$.

H. *Für den Typus* [2 1 1 1] *kommen als Ordnungen in Betracht*: $\mathfrak{M} = \mathfrak{L}_2$ (F_1, F_2 *eindeutig*); $\mathfrak{M} = \mathfrak{Z}'$ (F_1, F_2 9-*deutig*); $\mathfrak{M} = \mathfrak{X}_\varkappa$ (F_1, F_2 2-*deutig*); $\mathfrak{M} = \mathfrak{Z}'_\varkappa$ (F_1, F_2 18-*deutig*); $\mathfrak{M} = \mathfrak{R}_{\varkappa\beta}$ (F_1, F_2 4-*deutig*).

Mod $\mathfrak{L}_2$ erhalten wir wieder drei Möglichkeiten:

A:	$F_1 \equiv 0$,	$F_2 \equiv X$,	$F_3 \equiv -X-Y$,	$F_4 \equiv X-Y$
B:	0,	$-X$,	$-Y$,	$-Y$
C:	0,	0,	$X-Y$,	$-X-Y$.

[2 1 1 1]A: Relation (4) gibt auf F_2 angewandt: $XY \equiv 0$, auf F_3 oder F_4 angewandt: $X^2 + Y^2 \equiv (X \pm Y)^2 \equiv L_2(X \pm Y) \equiv K_1X^3 + K_2Y^3$. Es ist also $X^2 \approx Y^2$, woraus $X^3 \equiv Y^3 \equiv 0$ und $X^2 + Y^2 \equiv 0$ folgt. Relation (5) liefert auf F_1 angewandt: $f_1 \equiv 3 + X^2 \equiv 0$. Es ist also entweder $\mathfrak{M} = \mathfrak{L}_2$ oder $\mathfrak{M} = \mathfrak{Z}'$.

[2 1 1 1]B: Wieder gilt $XY \equiv 0$. $F_3(X+Y) \equiv 0$ ergibt $Y(X+Y) \equiv (X+Y)L_2$. Es gibt also ein $\varkappa > 2$, so daß $Y^2 \sim X^\varkappa$. Daraus folgt $Y^3 \equiv 0$. Relation (5) auf F_1 angewandt gibt $f_1 \equiv 0$. Es ist also $\mathfrak{M} = \mathfrak{X}_\varkappa$ oder $\mathfrak{M} = \mathfrak{Z}'_{\varkappa+1}$.

[2 1 1 1]C formen wir auf [3 3 4 3] um mit

$$F_1 \equiv Y, \quad F_2 \equiv -X, \quad F_3 \equiv F_4 \equiv 0 \bmod \mathfrak{L}_2.$$

Da (4) zufolge $XY < \mathfrak{L}_3$, können wir ansetzen:

$$F_1 \equiv -2Y - Y^2 + J_1X^{\varrho_1} + J_2Y^{\varrho_2}, \quad F_2 \equiv 2X + X^2 + J_3X^{\varrho_3} + J_4Y^{\varrho_4}, \quad \varrho_i \geqq 2, \text{ aber}$$

$$X^{\varrho_1}, \; X^{\varrho_3} \not\equiv 0(\mathfrak{M}, Y), \quad Y^{\varrho_2}, \; Y^{\varrho_4} \not\equiv 0(\mathfrak{M}, X), \tag{14}$$

weil S_1 und S_2 nicht kapitulieren. Aus (4) folgt dann:

$$XY \sim X^{\varrho_1+1} \sim Y^{\varrho_4+1}$$

und aus (5):

$$f_3 \sim Y^{\varrho_2+1} \sim X^{\varrho_3+1},$$

also wegen (14): $\varrho_1 = \varrho_3$; $\varrho_2 = \varrho_4$.

Ferner ist F_3 durch X und Y teilbar, also $F_3(X+Y) \equiv f_3 \equiv 0$. Wir erhalten daher $XY \equiv X^{\varrho_1+1} \equiv Y^{\varrho_2+1} \equiv f_3 \equiv 0$, was auf die Ordnung $\mathfrak{M} = \mathfrak{R}_{\varrho_1+1, \varrho_2+1}$ führt.

II.

Wir wollen jetzt auch für $\mathsf{P}(\sqrt{-3299})$ die Relativgruppe des zweiten Klassenkörpers bestimmen.

Bezeichnen wir in Kapitel 1, III die Klasse A mit S_1, die Klasse CA^{-3} mit S_2, so sind S_1 und S_2 Erzeugende der Klassengruppe mit $S_1^9 = S_2^3 = E$. Die vier kubischen Klassenkörper K_1, K_2, K_3 und K_4 gehören dann zu den Untergruppen

$$\{S_1\}, \quad \{S_1S_2\}, \quad \{S_1S_2^{-1}\} \text{ und } \quad \{S_2, S_1^3\}. \tag{15}$$

Zur Kapitulation können in diesen Körpern nur Klassen der Ordnung 3, also nur die Elemente der Gruppe $\{S_1^3, S_2\}$ gelangen, und zwar ist die Zuordnung, wie ausgerechnet wurde, folgende:

$$K_1 \to S_2, \; K_2 \to S_1^3, \; K_3 \to S_1^3S_2^{-1}, \; K_4 \to S_2. \tag{16}$$

Wir setzen wie in I den Kommutator $A = S_2^{-1}S_1^{-1}S_2S_1$, $X = S_1 - 1$, $Y = S_2 - 1$, außerdem $1 + S_1 + S_1^2 = f_1'$ und

$$S_1^9 = A^{F_1}, \; S_2^3 = A^{F_2}, \; (S_1^3S_2)^3 = A^{F_3}, \; (S_1^3S_2^2)^3 = A^{F_4}. \tag{17}$$

Dann besagen die Relationen (16) der Reihe nach:

$$X \mid F_2; \; X + Y + XY \mid F_1; \; X - Y \mid F_4; \; (Y, Xf_1') \mid F_2 + X + 3. \tag{18}$$

Nämlich für K_1 und K_3 liegen die kapitulierenden Klassen außerhalb der zugehörigen Untergruppen, weswegen die Verlagerungen dieser Klassen gleich ihren in (17) angeführten dritten Potenzen ausfallen. Aber auch für K_2 ist A^{F_1} die Verlagerung von S_1^3, da $S_1^{3(1+S_1+S_1^2)} = S_1^9$. Für K_4 aber lautet die Verlagerung: $S_2^{1+S_1+S_1^2} = A^{F_3+X+3}$. Die Exponenten dieser vier Verlagerungen müssen dann wirklich die in (18) angegebenen Teilbarkeiten aufweisen, weil

$$\{A^X\}, \; \{A^{X+Y+XY}\}, \; \{A^{X-Y}\}, \; \{A^Y, A^{Xf_1'}\} \tag{19}$$

die Kommutatorgruppen von (15) sind.

F_3 und F_4 lassen sich wieder wie in 2, I durch F_1 und F_2 ausdrücken, und zwar gilt hier, wenn T_1 und T_2 dieselben Ausdrücke wie in 2 I zwischen (9) und (10) bedeuten:

$$(20) \qquad \begin{array}{l} F_3 = F_1 + F_2 + f_1' T_1; \quad F_4 = F_1 + 2F_2 + f_1' T_2. \\ F_3 \equiv F_1 + F_2 \quad ; \quad F_4 \equiv F_1 - F_2 \pmod{\mathfrak{L}_2}. \end{array}$$

Denn unsere jetzigen F entstehen aus den früheren, indem man S_1 durch S_1^3 ersetzt, S_2 aber beläßt; dabei wird deren Kommutator A durch $A'' = S_2^{-1} S_1^{-3} S_2 S_1^3$ ersetzt.

Wir zeigen zuerst:

A. Die symbolische Ordnung $\mathfrak{M}$ von A ist durch $\mathfrak{L}_2$ teilbar.

α) Angenommen es sei $Y \equiv 0\ (\mathfrak{L}_2, \mathfrak{M})$, also nach (12) $Y \equiv 3R + QX^2\ (\mathfrak{M})$. Nach (5) gilt $X | f_2 = 3 + 3Y + Y^2 \equiv 3 + 9R + 9R^2 + QX^2$, also $X | 3 \bmod \mathfrak{M}$ und daher wegen (12) auch $X | Y$. Daraus würde aber folgen, daß in K_1 mehrfache Kapitulation stattfindet. Es gilt also $Y \not\equiv 0\ (\mathfrak{L}_2, \mathfrak{M})$.

β) Es sei X oder $X \pm Y \equiv 0\ (\mathfrak{L}_2, \mathfrak{M})$. Wir können uns auf die Widerlegung von $X \equiv 0\ (\mathfrak{L}_2, \mathfrak{M})$ beschränken. Zufolge (5) gilt $f_2 \equiv F_2 X$, also müßte $f_2 < \mathfrak{L}_3$ sein, wenn $X < \mathfrak{L}_2 \bmod \mathfrak{M}$; denn wegen $F_2 Y \equiv 0$ ist α) zufolge $F_2 \equiv 0\ (\mathfrak{L})$. Setzen wir $X \equiv 3R + QY^2\ (\mathfrak{M})$ ein, so ergibt das $3 + 3Y + Y^2 \equiv 0\ (9, 3Y, Y^3)$.[15]) Es wäre also $3 \sim Y^2$, und daraus folgte $Y | X \bmod \mathfrak{M}$. Dann müßte aber in K_4 mehrfache Kapitulation stattfinden.

Damit ist bewiesen, daß tatsächlich $\mathfrak{M} < \mathfrak{L}_2$ ist.

Wir beweisen sodann:

B. $\mathfrak{M} = \mathfrak{L}_2$.

Da $\mathfrak{M} < \mathfrak{L}_2$ ist, liefert jetzt (18) mod $\mathfrak{L}_2$:

$$F_1 \equiv a(X + Y), \quad F_2 \equiv bX \equiv -X + cY, \quad F_4 \equiv d(X - Y).$$

Nach (20) gilt dann:

$$a \equiv 1, \quad b \equiv -1, \quad c \equiv 0, \quad d \equiv -1, \quad \text{also}$$
$$F_1 \equiv X + Y, \quad F_2 \equiv -X, \quad F_3 \equiv Y, \quad F_4 \equiv -X + Y.$$

Da S_2 in K_2 kapituliert, können wir aus $F_2 \equiv -X$ die Beziehung $F_2 \sim X$ und zufolge (4) schließlich $XY \equiv 0$ schließen. Daraus und wieder mit Hilfe von (4) folgt: $(X + Y)X \equiv X^2 \equiv 0\ (\mathfrak{M})$ und $(X - Y)(S_1^3 - S_2) = (X - Y)(f_1' X - Y) \equiv Y^2 \equiv 0\ (\mathfrak{M})$, außerdem $3 \equiv f_2 \equiv LX \equiv 0$.

Es ist also $\mathfrak{M} = \mathfrak{L}_2$, und die obigen Kongruenzen für die F_i gelten mod $\mathfrak{M}$ selbst. Daraus läßt sich leicht die Kapitulation für die Zwischenkörper 9. Grades übersehen: In allen drei zyklischen, aber auch im nicht zyklischen Körper 9. Grades geht die Untergruppe $\{S_1^3, S_2\}$ in die Hauptklasse über. S_1 wird erst im Klassenkörper selbst zur Hauptklasse.

3. Der Klassenkörperturm.

Wir wollen jetzt zeigen, daß der 3-Klassenkörperturm von $\mathsf{P}(\sqrt{-4027})$ und $\mathsf{P}(\sqrt{-3299})$ mit dem zweiten Klassenkörper endigt.

Dazu beweisen wir den folgenden allgemeinen Satz für zweistufige Gruppen:

Die zweistufige Gruppe $\mathfrak{H}$, deren Ordnung eine Potenz von 3 ist, besitze die zwei Erzeugenden S_1 und S_2, der Kommutator A von S_1 und S_2 habe die symbolische Ordnung $\mathfrak{L}_2$. Lassen sich außerdem alle Elemente der Gruppe $\{A^X, A^Y\}$ aus den dritten Potenzen der Elemente von $\mathfrak{H}$ erzeugen, so kann $\mathfrak{H}$ nicht maximale zweistufige Faktorgruppe einer umfassenderen Gruppe sein, deren Ordnung ebenfalls eine Potenz von 3 ist.

[15]) (11) ist hier nicht gültig.

Die letzte Voraussetzung dieses Satzes ist bei allen Gruppen vom Typus (3, 3) und auch bei $P(\sqrt{-3299})$ erfüllt. (Siehe Kap. 2.)

Zum Beweise genügt es zu zeigen, daß $\mathfrak{H}$ nicht Faktorgruppe einer dreistufigen Gruppe sein kann. Wir nehmen an, $\mathfrak{H}$ sei Faktorgruppe in einer dreistufigen Gruppe $\mathfrak{G}$, und unterscheiden dann zwei Fälle:

1) Die zweite Kommutatorgruppe $\mathfrak{G}''$ von $\mathfrak{G}$, die Kommutatorgruppe der Kommutatorgruppe $\mathfrak{G}'$, habe die Eigenschaft, daß $\mathfrak{G}'' = \mathfrak{G}''^{\mathfrak{L}}$, wo $\mathfrak{G}''^{\mathfrak{L}}$ die Menge aller Elemente C^L bedeutet, für welche $C < \mathfrak{G}''$ und $L < (3, X, Y)$ ist. Wir zeigen, daß aus dieser Voraussetzung folgt: $\mathfrak{G}'' = E$.

Behauptung 1) ergibt sich aus dem folgenden allgemeineren für beliebige Primzahlen l gültigen Satze:

Ist $\mathfrak{G}$ eine höchstens dreistufig-metabelsche Gruppe von Primzahlpotenzordnung l^m, und lassen sich alle Elemente C der zweiten Kommutatorgruppe $\mathfrak{G}''$ durch die l-ten Potenzen von Elementen C und Kommutatoren der C mit beliebigen Elementen aus $\mathfrak{G}$ ausdrücken, so ist $\mathfrak{G}$ höchstens zweistufig.

Der Satz gilt entsprechend für n-stufige Gruppen. Der folgende Beweis ist so durchgeführt, daß er ohne weiteres einen vollständigen Induktionsschluß von $(n-1)$-stufigen Gruppen auf n-stufige zuläßt.

Zunächst gilt der entsprechende Satz für zweistufige Gruppen $\overline{\mathfrak{G}}$: aus $\overline{\mathfrak{G}}' = \overline{\mathfrak{G}}'^{\overline{\mathfrak{L}}}$ folgt $\overline{\mathfrak{G}}' = E$, wenn $\overline{\mathfrak{L}} = (l, \overline{S} - 1)$ und $\overline{S}$ die Elemente von $\overline{\mathfrak{G}}$ durchläuft [16]). Setzen wir hier $\overline{\mathfrak{G}} = \mathfrak{G}'$, so folgt: $\mathfrak{G}'' = E$, wenn $\mathfrak{G}'' = \mathfrak{G}''^{\mathfrak{L}'}$, wo jetzt $\mathfrak{L}' = (l, A - 1)$ und A die Gesamtheit aller Elemente von $\mathfrak{G}'$ durchläuft. Nun wollen wir aber $\mathfrak{G}'' = E$ schon aus $\mathfrak{G}'' = \mathfrak{G}''^{\mathfrak{L}}$ mit $\mathfrak{L} = (l, S - 1)$ schließen — im allgemeinen gilt $\mathfrak{G}'' > \mathfrak{G}''^{\mathfrak{L}} > \mathfrak{G}''^{\mathfrak{L}'} > E$ — es bleibt darum der Nachweis von $\mathfrak{G}''^{\mathfrak{L}} = \mathfrak{G}''^{\mathfrak{L}'}$ oder, daß in der Faktorgruppe $\mathfrak{G}/\mathfrak{G}''^{\mathfrak{L}'}$ schon $\mathfrak{G}'' = E$ für $\mathfrak{G}'' = \mathfrak{G}''^{\mathfrak{L}}$ gilt. Wir brauchen also unseren Satz nur für $\mathfrak{G}''^{\mathfrak{L}'} = E$ zu beweisen, und das hat den Vorteil, daß dann die symbolischen Exponenten $F(S)$ der C einen kommutativen Ring bilden ($C^A = C$, $C^{S_1 S_2} = C^{S_2 S_1}$). Jetzt können wir den Beweis entsprechend wie in [16]) führen: Angenommen, es sei in $\mathfrak{G}''$ jedes Element C in der Gestalt $C = \prod C_\varrho^{L_\varrho}$ darstellbar, wo $L_\varrho < \mathfrak{L}$ und jedes C_ϱ wieder in $\mathfrak{G}''$ liegt, so gilt dasselbe für jedes C_ϱ, und man erhält durch Iteration des Prozesses, daß für beliebiges k jedes C in der Form $C = \prod C_\varrho^{(k) L_\varrho^{(k)}}$ darstellbar ist, wo $C_\varrho^{(k)} < \mathfrak{G}''$ und $L_\varrho^{(k)} < \mathfrak{L}^k$. Für genügend hohes k sind alle $L_\varrho^{(k)}$ entweder durch l oder durch Differenzen $(S-1)^h$ teilbar, und für genügend hohes h sind die symbolischen Potenzen $C^{(S-1)^h}$ Potenzen von C^l. Sind aber in einer Gruppe von l-Potenzordnung alle Elemente l-te Potenzen, so besteht die Gruppe nur aus dem Einheitselement.

2) Es sei $\mathfrak{G}'' \neq \mathfrak{G}^{\mathfrak{L}}$. In diesem Falle dürfen wir jetzt, nachdem 1) bewiesen ist, voraussetzen, daß $\mathfrak{G}''$ dem Zentrum angehört und kein Element der Ordnung 9 enthält. $\mathfrak{G}''$ wird symbolisch sicher schon aus den Kommutatoren der Erzeugenden A, A^X, A^Y von $\mathfrak{G}'$ erzeugt, also aus $C_{1x} = (A^X, A)$, $C_{1y} = (A^Y, A)$ und $C_{xy} = (A^Y, A^X)$. Hierbei verwenden wir allgemein die Bezeichnungsweise für Kommutatoren:

$$(S, T) = S^{-1} T^{-1} S T = S^{-1+T},$$

insbesondere

$$(A, S_1) = A^{-1+S_1} = A^X, \quad (A, S_2) = A^{-1+S_2} = A^Y.$$

(Die Addition der Exponenten ist im allgemeinen nicht kommutativ; wir präzisieren darum $X = -1 + S_1$, $Y = -1 + S_2$, in dieser Reihenfolge der Summanden.)

---

[16]) Siehe Scholz, Heidelbg. Ak. Ber. 1933, Nr. 2.

Für die Kommutatoren gelten dann die folgenden Rechenregeln:

$$(RS,\ T) = (R,\ T)^S\,(S,\ T)$$
$$(S,\ TU) = (S,\ T)\,(S^T,\ U), \quad \text{und für} \quad U = T^{-1}:$$
$$(S,\ T^{-1}) = (S,\ T)^{-T^{-1}}.$$

Wir beweisen nun:

a) $C_{xy} = E$. Es ist nämlich

$$(A^Y, A^X) = (A^Y, A^{-1})\,(A^{YA^{-1}}, A^{S_1}) = C_{1y}^{-A^{-1}}(A^{YA^{-1}S_1^{-1}}, A)^{S_1} = C_{1y}^{-1}C_{1y}^{S_1} = E,$$

wenn man berücksichtigt, daß $\mathfrak{G}''$ dem Zentrum angehören soll, woraus folgt, daß der Kommutator zweier Elemente nur von ihren Restklassen mod $\mathfrak{G}''$ abhängt. Nun ist $A^{YA^{-1}S_1^{-1}} \equiv A^{YS_1^{-1}} \equiv A^Y \pmod{\mathfrak{G}''}$ wegen $A^{YX} < \mathfrak{G}''$.

b) $\qquad (A, S^3) = E \quad$ für beliebiges $S < \mathfrak{G}$.

Setzen wir $\Delta = -1 + S$, so ist

$$(A, S^3) = (A, S)^{1+S+S^2} = A^{\Delta(1+S+S^2)} = A^{\Delta(2+\Delta+1+\Delta+S\Delta)} = A^{\Delta 3+\Delta^2 2}(A^{\Delta^2}, A^\Delta)^{A^{2\Delta^2}}A^{\Delta S\Delta}$$
$$= A^{\Delta 3+\Delta^2 3+\Delta^3} = A^{\Delta 3} = A^{-1}A^SA^{-1}A^SA^{-1}A^S = A^{-3}A^{3S}(A^S, A^{-1})^3 = A^{3(-1+S)} = E.$$

Wenn nun wie bei unserer Gruppe $\mathfrak{H}$ die Kommutatoren A^X und A^Y durch die S^3 ausdrückbar sind, gilt dann auch:

$$(A^X, A) = (A^Y, A) = E.$$

Damit ist 2) bewiesen.

Anschließend geben wir noch kurz an, wie man auch für $\mathsf{P}(\sqrt{-9748})$ zeigen kann, daß der Klassenkörperturm mit dem zweiten Klassenkörper endigt.

Um zu beweisen, daß $\mathfrak{G}'' = E$ ist, dürfen wir wieder $\mathfrak{G}''^2 = E$ annehmen. Beachtet man nun, daß dann $(A^{3F_1}, A^{F_1}) = (A^{F_1}, A^{F_1})^3 = E$ wird — man kann statt mit 3 wieder allgemeiner mit l operieren; die bei der Ausrechnung dieses Kommutators hinzukommenden Kommutatoren liegen wieder alle in $\mathfrak{G}''^2$ — und daß $(\mathfrak{M}, 3) = \mathfrak{L}_2$ ist, wenn $\mathfrak{M} = (X^\alpha, f_1, XY, Y^2)$ die symbolische Ordnung der zweiten Klassengruppe für $D = -9748$ ist, so bleiben wieder nur die Kommutatoren C_{1x}, C_{1y} und C_{xy} zu untersuchen. Man beweist dann auf dieselbe Weise wie oben für die Gruppe $\mathfrak{H}$, daß diese drei Kommutatoren die Identität ergeben.

Erwähnt sei noch, daß hier $\alpha = 4$ ausfällt: Nach der unter [2] zitierten Note muß $\alpha = 2\gamma$ ausfallen, und die Klassengruppe des einen absolut kubischen Körpers mit der Diskriminante $D = -9748$ ist dann eine zyklische Gruppe der Ordnung 3^γ, während die anderen drei überhaupt nur eine Klassengruppe der Ordnung 3 besitzen. Der bevorzugte kubische Körper ist der bei unserer Bezeichnung zu S_2 gehörige mit der Gleichung: $x^3 - 30x - 1028 = 0$. Nun braucht man aber nach einem bekannten Minkowskischen Kriterium nur wenige Ideale $\mathfrak{j}$ (mit einer Norm $\leqq 21$) daraufhin zu prüfen, daß sie nicht erst in 27-ter Potenz Hauptideale werden, was am leichtesten durch Betrachtung der Normen geschieht. Dann hat man die Gewißheit, daß es überhaupt keine solchen Ideale gibt, daß also $\gamma = 2$, $\alpha = 4$. Damit ist nun auch die Gruppe des vollen Klassenkörperturms von $\mathsf{P}(\sqrt{-9748})$ bekannt.

Eingegangen 31. Juli 1933.

Über die Definition der Zeuthen-Segreschen Invariante.

Von *M. Oehlert* in Merseburg.

Inhaltsverzeichnis.

Einleitung 42
I. Wie $\mathfrak{X}$ von $\langle \mathfrak{G} \rangle$ abhängt 44
II. Wie ϑ von $\langle \mathfrak{G} \rangle$ abhängt. Beitrag der Stellen, die nicht feste Stellen von $\langle \mathfrak{G} \rangle$ sind 45
III. Wie ϑ von $\langle \mathfrak{G} \rangle$ abhängt. Beitrag der festen Stellen von $\langle \mathfrak{G} \rangle$ 47
1) Vorbetrachtung 47
2) Formel für $(U, V)_0$ 48
3) Bestimmung von $(\mathfrak{D}, \mathfrak{G}_a^2\, dw/d\mathfrak{G}_a)_0$ 49
4) Berechnung von $\Sigma\beta_k$ 50
5) Berechnung von $\Sigma\alpha_k$ 52
IV. Definition der Zeuthen-Segreschen Invariante 53

Einleitung.

Es sei F eine algebraische Fläche. Wir bezeichnen den zugehörigen algebraischen Körper zweier unabhängigen Veränderlichen auch mit F. Es sei $\langle \mathfrak{G} \rangle$ eine eindimensionale lineare Kurvenschar auf der Fläche F. Das Geschlecht einer allgemeinen Kurve der Schar sei π, die Zahl der Schnittpunkte zweier Kurven der Schar sei N, und die Zahl derjenigen Kurven der Schar, die einen Doppelpunkt haben, sei δ. Dann ist die Zahl

$$Z = \delta - 4\pi - N \tag{1}$$

eine Invariante der Fläche, d. h. unabhängig von der Wahl der Schar $\langle \mathfrak{G} \rangle$.

Sind $\mathfrak{G}_1$ und $\mathfrak{G}_2$ zwei Kurven der Schar $\langle \mathfrak{G} \rangle$, so ist $w = \mathfrak{G}_1/\mathfrak{G}_2$ eine Funktion des Körpers, und $\langle \mathfrak{G} \rangle$ kann definiert werden durch

$$w = \xi,$$

wo ξ einen Parameter bedeutet. F. Severi ist auf den Gedanken gekommen, für w ein lineares Integral des Körpers zu nehmen. Es zeigt sich, daß man auch für solche Kurvenscharen eine Invariante definieren kann, die im Wesentlichen die Zeuthen-Segresche ist. H. W. E. Jung zeigte dann, daß man einfacher lineare Differentiale $Adx + Bdy$, die nicht total zu sein brauchen, benutzt. In der Darstellung von Jung sieht die Severische Entdeckung folgendermaßen aus:

Ein Differential

$$dw = Adx + Bdy$$

können wir in der Umgebung einer Stelle S in der Form schreiben

$$dw = \mathfrak{X}(Udu + Vdv),$$

wo $\mathfrak{X}$ die zugeordnete Funktion eines gleich bezeichneten Divisors $\mathfrak{X}$ ist, während U und V gewöhnliche Potenzreihen der Ortsuniformisierenden u und v sind, die bei S teilerfremd sind. Die Zahl der Schnittpunkte der Kurven $U = 0$ und $V = 0$ in S sei mit ϑ_0 bezeichnet; und es sei $\sum_S \vartheta_0 = \vartheta$ gesetzt, wo über alle Stellen S zu summieren ist. Bezeichnet

$(\mathfrak{K})$ die kanonische Klasse von F und $(\mathfrak{X}') = (\mathfrak{K}\mathfrak{X}^{-1})$ die Ergänzungsklasse von $(\mathfrak{X})$, so ist die Zahl

$$\vartheta + (\mathfrak{X}, \mathfrak{X}') = I$$

unabhängig von der Wahl des Differentials dw. Der Beweis von Jung ist folgender:

Es seien

$$dw_1 = A_1 dx + B_1 dy = \mathfrak{X}_1(U_1 du + V_1 dv),$$
$$dw_2 = A_2 dx + B_2 dy = \mathfrak{X}_2(U_2 du + V_2 dv)$$

zwei Differentiale. ϑ_1 und ϑ_2 seien die Zahlen ϑ für diese Differentiale. Es ist identisch

$$(A_1 B_2 - A_2 B_1) dx dy = \mathfrak{X}_1 \mathfrak{X}_2 (U_1 V_2 - U_2 V_1)\, du dv.$$

Es sei gesetzt

$$\mathfrak{T} = U_1 V_2 - U_2 V_1. \tag{2}$$

Ist $\mathfrak{Z}$ der Verzweigungsdivisor inbezug auf x und y, und sind $\mathfrak{L}$ und $\mathfrak{M}$ die Nenner von x und y, so ist

$$dx dy = \mathfrak{Z}\mathfrak{L}^{-2}\mathfrak{M}^{-2} du dv$$

und daher

$$\mathfrak{X}_1 \mathfrak{X}_2 \mathfrak{T} = \mathfrak{X}_1 \mathfrak{X}_2 (U_1 V_2 - U_2 V_1) = (A_1 B_2 - A_2 B_1) \frac{\mathfrak{Z}}{\mathfrak{L}^2 \mathfrak{M}^2}.$$

Es ist daher $\mathfrak{T}$ zugeordnete Funktion eines Divisors $\mathfrak{T}$. Da $\mathfrak{Z}\mathfrak{L}^{-2}\mathfrak{M}^{-2} \sim \mathfrak{K}$, und da als Funktion des Körpers F $(A_1 B_2 - A_2 B_1) \sim 1$, so folgt

$$\mathfrak{X}_1 \mathfrak{X}_2 \mathfrak{T} \sim \mathfrak{K}. \tag{3}$$

Für $\mathfrak{T} = 0$, d. h. im algebraischen Körper $\mathfrak{T}$ einer unabhängigen Veränderlichen, ist

$$\frac{dw_1}{dw_2} = \frac{\mathfrak{X}_1 U_1}{\mathfrak{X}_2 U_2} = \frac{\mathfrak{X}_1 V_1}{\mathfrak{X}_2 V_2} = r,$$

wo r eine Funktion des Körpers $\mathfrak{T}$ ist. Die Beiträge, die S zur Ordnung des Zählers und des Nenners von r liefert, sind

$$g_0 = (\mathfrak{X}_1 U_1, \mathfrak{T})_0 \quad \text{und} \quad h_0 = (\mathfrak{X}_2 U_2, \mathfrak{T})_0,$$

wenn wir allgemein mit $(\mathfrak{P}, \mathfrak{Q})_0$ die Zahl der Schnittpunkte der Kurven $\mathfrak{P}$ und $\mathfrak{Q}$ in S bezeichnen. Es wird also

$$g_0 - h_0 = (\mathfrak{X}_1, \mathfrak{T})_0 - (\mathfrak{X}_2, \mathfrak{T})_0 + (U_1, \mathfrak{T})_0 - (U_2, \mathfrak{T})_0.$$

Andrerseits folgt aus (2) für $U_1 = 0$

$$(\mathfrak{T}, U_1)_0 = (U_1, U_2)_0 + (U_1, V_1)_0$$

und für $U_2 = 0$

$$(\mathfrak{T}, U_2)_0 = (U_1, U_2)_0 + (U_2, V_2)_0,$$

woraus durch Subtraktion folgt

$$(\mathfrak{T}, U_1)_0 - (\mathfrak{T}, U_2)_0 = (U_1, V_1)_0 - (U_2, V_2)_0 = \vartheta_{10} - \vartheta_{20}.$$

Daher wird

$$g_0 - h_0 = (\mathfrak{X}_1, \mathfrak{T})_0 - (\mathfrak{X}_2, \mathfrak{T})_0 + \vartheta_{10} - \vartheta_{20}.$$

Summieren wir über alle Stellen S, so wird

$$g - h = (\mathfrak{X}_1, \mathfrak{T}) + \vartheta_1 - (\mathfrak{X}_2, \mathfrak{T}) - \vartheta_2 = 0;$$

denn da r eine Funktion des algebraischen Körpers $\mathfrak{T}$ ist, ist die Zahl der Nullstellen g gleich der Zahl der Unendlichkeitsstellen h. Es ist also

$$(\mathfrak{X}_1, \mathfrak{T}) + \vartheta_1 = (\mathfrak{X}_2, \mathfrak{T}) + \vartheta_2. \tag{4}$$

Wegen (3) ist

$$(\mathfrak{X}_1, \mathfrak{T}) = (\mathfrak{X}_1, \mathfrak{K}) - (\mathfrak{X}_1, \mathfrak{X}_1) - (\mathfrak{X}_1, \mathfrak{X}_2),$$
$$(\mathfrak{X}_2, \mathfrak{T}) = (\mathfrak{X}_2, \mathfrak{K}) - (\mathfrak{X}_2, \mathfrak{X}_2) - (\mathfrak{X}_1, \mathfrak{X}_2).$$

Die Gleichung (4) nimmt also die Form an

$$\vartheta_1 + (\mathfrak{X}_1, \mathfrak{K}) - (\mathfrak{X}_1, \mathfrak{X}_1) = \vartheta_2 + (\mathfrak{X}_2, \mathfrak{K}) - (\mathfrak{X}_2, \mathfrak{X}_2).$$

Der Ausdruck

$$I = \vartheta + (\mathfrak{X}, \mathfrak{K}) - (\mathfrak{X}, \mathfrak{X}) = \vartheta + (\mathfrak{X}, \mathfrak{X}') \tag{5}$$

ist also eine Invariante des Körpers F.

Wie Severi gezeigt hat, ist $I = Z + 4$. Es liegt daher nahe, die Invariante I für das totale Differential dw einer Funktion w des Körpers F zu berechnen, um damit eine Definition von Z zu erhalten, die in allen Fällen gilt. Denn die oben gegebene Definition von Z versagt, wenn die Kurven der Schar $\langle \mathfrak{G} \rangle$ mehrfache Schnittpunkte haben, oder wenn es in $\langle \mathfrak{G} \rangle$ Kurven gibt, die mehrfache Punkte oder mehrfache Faktoren haben. Man kommt so zu einer in allen Fällen geltenden Definition von Z auf einfachere und übersichtlichere Art als die von Jung in seiner Arbeit in den Rendiconti del Circolo Matematico di Palermo, Bd. XXXIV (1912) benutzte. Außerdem ergibt sich ein Beweis für die Gleichung $I = Z + 4$.

Es ist der Zweck der folgenden Arbeit, das genauer auszuführen. Es sei also

$$w = \frac{\mathfrak{G}_0}{\mathfrak{G}_a}$$

eine Funktion des Körpers F. Wir wollen die Invariante I des Differentials dw berechnen, und zwar unter Benutzung von Größen, die sich auf die Kurven der Schar $\langle \mathfrak{G} \rangle$, nämlich

$$\mathfrak{G} = \mathfrak{G}_0 - \xi \mathfrak{G}_a,$$

beziehen. Wir können und wollen voraussetzen, daß $\mathfrak{G}_a$ eine allgemeine Kurve der Schar ist, also keine Besonderheiten hat. Es ist

$$dw = d(w - \xi) = \frac{\mathfrak{G}_a d\mathfrak{G} - \mathfrak{G} d\mathfrak{G}_a}{\mathfrak{G}_a^2}, \tag{6}$$

und bei einer Stelle S

$$dw = \mathfrak{x}(Udu + Vdv).$$

1. Wie $\mathfrak{x}$ von $\langle \mathfrak{G} \rangle$ abhängt.

Zunächst folgt aus (6), daß wir setzen können

$$\mathfrak{x} = \frac{\mathfrak{T}}{\mathfrak{G}_a^2},$$

wo dann $\mathfrak{T}$ ein ganzer Divisor ist. Es sei ferner $\mathfrak{G}$ eine Kurve aus $\langle \mathfrak{G} \rangle$, und es sei in Primteiler zerlegt

$$\mathfrak{G} = \mathfrak{P}_1^{\alpha_1} \mathfrak{P}_2^{\alpha_2} \cdots \mathfrak{P}_\varrho^{\alpha_\varrho}.$$

Dann ist der Beitrag, den diese Kurve $\mathfrak{G}$ zu $\mathfrak{T}$ liefert,

$$\mathfrak{T}_\mathfrak{G} = \mathfrak{P}_1^{\alpha_1 - 1} \mathfrak{P}_2^{\alpha_2 - 1} \cdots \mathfrak{P}_\varrho^{\alpha_\varrho - 1}.$$

Die Richtigkeit dieser Behauptung werde z. B. gezeigt für den Primteiler $\mathfrak{P}_1$.

Wir wählen eine Stelle S so, daß $\mathfrak{P}_1$ durch S geht und dort regulär ist, daß aber $\mathfrak{G}_a$ und die $\mathfrak{P}_2, \ldots, \mathfrak{P}_\varrho$ nicht durch S gehen. Dann können wir annehmen

$$\mathfrak{P}_1 = u; \quad \mathfrak{G}_a = \mathfrak{P}_2 = \cdots = \mathfrak{P}_\varrho = 1,$$

sodaß

$$w - \xi = \mathfrak{G} = cu^{\alpha_1}, \quad dw = c\alpha_1 u^{\alpha_1 - 1} du + 0 \cdot dv.$$

Also wird

$$\mathfrak{x} = u^{\alpha_1 - 1} = \mathfrak{P}_1^{\alpha_1 - 1}.$$

Und umgekehrt: der Primteiler $\mathfrak{P}$ sei in $\mathfrak{X}$ in der Potenz $\alpha - 1$ enthalten. S sei eine Stelle, durch die $\mathfrak{P}$ geht und wo $\mathfrak{P}$ regulär ist. S liege nicht auf $\mathfrak{G}_a$. Wir können für S also annehmen

$$\mathfrak{G}_a = 1; \quad \mathfrak{P} = u; \quad \mathfrak{X} = u^{\alpha-1}.$$

In $w - \xi = \mathfrak{G}$ sei das ξ so gewählt, daß $\mathfrak{G}$ durch S geht. Wegen $\mathfrak{X} = u^{\alpha-1}$ muß

$$dw = \frac{\partial \mathfrak{G}}{\partial u} du + \frac{\partial \mathfrak{G}}{\partial v} dv$$

durch $u^{\alpha-1}$ teilbar sein, d. h. $\frac{\partial \mathfrak{G}}{\partial u}$ und $\frac{\partial \mathfrak{G}}{\partial v}$ müssen den Faktor $u^{\alpha-1}$ enthalten. $\mathfrak{G}$ muß also die Form haben

$$\mathfrak{G} = b_0 + b_1 u^{\alpha} + \cdots,$$

wo die b_i Funktionen von v sind. Weil auch $\frac{\partial \mathfrak{G}}{\partial v}$ durch $u^{\alpha-1}$ teilbar sein soll, muß b_0 konstant sein, und da $\mathfrak{G}$ durch S geht, also $\mathfrak{G}(0, 0) = 0$, ist $b_0 = 0$. Also ist $\mathfrak{G}$ durch $\mathfrak{P}^{\alpha}$ teilbar. Es ist daher

$$\mathfrak{X} = \frac{\mathfrak{P}_1^{\alpha_1-1}\, \mathfrak{P}_2^{\alpha_2-1} \cdots \mathfrak{P}_r^{\alpha_r-1}}{\mathfrak{G}_a^2} \tag{7}$$

wo die $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_r$ alle die Primteiler sind, die in irgendeiner Kurve der Schar $\langle \mathfrak{G} \rangle$ mehrfach vorkommen.

II. Wie ϑ von $\langle \mathfrak{G} \rangle$ abhängt.

Beitrag der Stellen, die nicht feste Stellen von $\langle \mathfrak{G} \rangle$ sind.

Wir betrachten zunächst den Fall, daß S keine der festen Stellen der Kurvenschar $\langle \mathfrak{G} \rangle$ ist. Als $\mathfrak{G}_a$ wählen wir dann eine allgemeine Kurve aus $\langle \mathfrak{G} \rangle$, die nicht durch S geht, sodaß wir bei S $\mathfrak{G}_a = 1$ annehmen können. Dann vereinfacht sich dw zu

$$dw = d\mathfrak{G} = \mathfrak{X}(U du + V dv),$$

und dabei ist nach (7)

$$\mathfrak{X} = \mathfrak{P}_1^{\alpha_1-1}\, \mathfrak{P}_2^{\alpha_2-1} \cdots \mathfrak{P}_\varrho^{\alpha_\varrho-1},$$

da die zugeordneten Funktionen der nicht in $\mathfrak{G}$ enthaltenen Primteiler $\mathfrak{P}_i$ gleich 1 angenommen werden können. Den Divisor

$$\frac{\mathfrak{G}}{\mathfrak{X}} = \mathfrak{P}_1\, \mathfrak{P}_2 \cdots \mathfrak{P}_\varrho$$

bezeichnen wir mit $\mathfrak{G}'$, sodaß

$$\mathfrak{G} = \mathfrak{X}\mathfrak{G}'$$

ist. Durch logarithmische Differentiation von $\mathfrak{G}$ folgt

$$\frac{d\mathfrak{G}}{\mathfrak{G}} = \alpha_1 \frac{d\mathfrak{P}_1}{\mathfrak{P}_1} + \alpha_2 \frac{d\mathfrak{P}_2}{\mathfrak{P}_2} + \cdots + \alpha_\varrho \frac{d\mathfrak{P}_\varrho}{\mathfrak{P}_\varrho}$$

oder

$$d\mathfrak{G} = \mathfrak{X}\mathfrak{G}' \left\{ \alpha_1 \frac{d\mathfrak{P}_1}{\mathfrak{P}_1} + \alpha_2 \frac{d\mathfrak{P}_2}{\mathfrak{P}_2} + \cdots + \alpha_\varrho \frac{d\mathfrak{P}_\varrho}{\mathfrak{P}_\varrho} \right\}$$

und

$$U = \mathfrak{G}' \left\{ \frac{\alpha_1}{\mathfrak{P}_1} \frac{\partial \mathfrak{P}_1}{\partial u} + \frac{\alpha_2}{\mathfrak{P}_2} \frac{\partial \mathfrak{P}_2}{\partial u} + \cdots + \frac{\alpha_\varrho}{\mathfrak{P}_\varrho} \frac{\partial \mathfrak{P}_\varrho}{\partial u} \right\}, \tag{8}$$

$$V = \mathfrak{G}' \left\{ \frac{\alpha_1}{\mathfrak{P}_1} \frac{\partial \mathfrak{P}_1}{\partial v} + \frac{\alpha_2}{\mathfrak{P}_2} \frac{\partial \mathfrak{P}_2}{\partial v} + \cdots + \frac{\alpha_\varrho}{\mathfrak{P}_\varrho} \frac{\partial \mathfrak{P}_\varrho}{\partial v} \right\}. \tag{9}$$

Ferner ist

$$\frac{\partial \mathfrak{G}'}{\partial u} = \mathfrak{G}'\left\{\frac{1}{\mathfrak{P}_1}\frac{\partial \mathfrak{P}_1}{\partial u} + \frac{1}{\mathfrak{P}_2}\frac{\partial \mathfrak{P}_2}{\partial u} + \cdots + \frac{1}{\mathfrak{P}_\varrho}\frac{\partial \mathfrak{P}_\varrho}{\partial u}\right\}, \tag{10}$$

$$\frac{\partial \mathfrak{G}'}{\partial v} = \mathfrak{G}'\left\{\frac{1}{\mathfrak{P}_1}\frac{\partial \mathfrak{P}_1}{\partial v} + \frac{1}{\mathfrak{P}_2}\frac{\partial \mathfrak{P}_2}{\partial v} + \cdots + \frac{1}{\mathfrak{P}_\varrho}\frac{\partial \mathfrak{P}_\varrho}{\partial v}\right\}. \tag{11}$$

Wir zeigen, daß

$$\vartheta_0 = (U, V)_0 = \left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0.$$

Die Potenzreihe $\mathfrak{P}_k(u, v)$ beginne mit Gliedern der Dimension q_k. Wir können und wollen annehmen, daß in $\mathfrak{P}_k(u, v)$ das Glied mit v^{q_k} vorkommt. Da es bei der Berechnung von Schnittpunktzahlen auf einen konstanten Faktor nicht ankommt, können wir annehmen, daß der Faktor von v^{q_k} in $\mathfrak{P}_k(u, v)$ gleich 1 ist. Setzen wir

$$q_1 + q_2 + \cdots + q_\varrho = q,$$

so beginnen V und $\frac{\partial \mathfrak{G}'}{\partial v}$ mit Gliedern der Dimension $q - 1$, und die Faktoren von v^{q-1} sind

$$\alpha_1 q_1 + \alpha_2 q_2 + \cdots + \alpha_\varrho q_\varrho \quad \text{und} \quad q,$$

also gewiß nicht Null.

Für $\mathfrak{P}_k = 0$ wird wegen (9) und (11)

$$V = \alpha_k \frac{\partial \mathfrak{G}'}{\partial v},$$

also

$$(V, \mathfrak{P}_k)_0 = \left(\frac{\partial \mathfrak{G}'}{\partial v}, \mathfrak{P}_k\right)_0$$

und nach Summation über alle $\mathfrak{P}_k$ $(k = 1, 2, \ldots \varrho)$

$$(V, \mathfrak{G}')_0 = \left(\frac{\partial \mathfrak{G}'}{\partial v}, \mathfrak{G}'\right)_0. \tag{12}$$

Die Gleichung $V = 0$ habe bei S die Lösungen

$$v = v_1, v_2, \ldots, v_l,$$

wo die v_i $(i = 1, 2, \ldots, l)$ gewöhnliche Potenzreihen von $u^{\frac{1}{\lambda_i}}$ sind, die für $u = 0$ verschwinden. Dann ist

$$\sum_{i=1}^{l} \lambda_i = q - 1. \tag{13}$$

Setzen wir die Lösungen $v = v_i$ in $\mathfrak{G}(u, v)$ ein, so sei

$$\mathfrak{G}(u, v_i) = \mathfrak{g}_i(u) = u^{\frac{\varrho_i}{\lambda_i}} e_i(u).$$

Dabei bedeutet hier wie im folgenden e immer eine Einheit. Dann ist nach der Definition der Schnittpunktzahlen

$$\sum_{i=1}^{l} \varrho_i = (\mathfrak{G}, V)_0. \tag{14}$$

Unter Berücksichtigung von $V(u, v_i) = 0$ wird

$$\frac{d\mathfrak{g}_i}{du} = \mathfrak{X}(u, v_i)\, U(u, v_i) = u^{\frac{\varrho_i - \lambda_i}{\lambda_i}} e_{i1}(u).$$

Daraus folgt unter Benutzung von (13) und (14)

$$(\mathfrak{X}, V)_0 + (U, V)_0 = \sum_{i=1}^{l} \varrho_i - \sum_{i=1}^{l} \lambda_i = (\mathfrak{G}, V)_0 - (q - 1);$$

und da wegen $\mathfrak{G} = \mathfrak{G}'\mathfrak{X}$ auch

$$(\mathfrak{G}, V)_0 = (\mathfrak{G}', V)_0 + (\mathfrak{X}, V)_0,$$

so ist

$$(U, V)_0 = (\mathfrak{G}', V)_0 - q + 1. \tag{15}$$

Es habe ferner $\frac{\partial \mathfrak{G}'}{\partial v} = 0$ bei S die Lösungen

$$v = v^{(1)}, v^{(2)}, \ldots, v^{(m)},$$

wo die $v^{(j)}$ $(j = 1, 2, \ldots, m)$ gewöhnliche Potenzreihen von $u^{\frac{1}{\mu_j}}$ sind, die für $u = 0$ verschwinden. Es ist dann

$$\sum_{j=1}^{m} \mu_j = q - 1. \tag{16}$$

Setzen wir die Lösungen $v = v^{(j)}$ in $\mathfrak{G}'(u, v)$ ein, so sei

$$\mathfrak{G}'(u, v^{(j)}) = \mathfrak{g}'^{(j)}(u) = u^{\frac{\sigma_j}{\mu_j}} e^{(j)}(u).$$

Dann ist also

$$\sum_{j=1}^{m} \sigma_j = \left(\mathfrak{G}', \frac{\partial \mathfrak{G}'}{\partial v}\right)_0. \tag{17}$$

Da $\frac{\partial \mathfrak{G}'}{\partial v}(u, v^{(j)}) = 0$ ist, so wird

$$\frac{\partial \mathfrak{G}'}{\partial u}(u, v^{(j)}) = \frac{d\mathfrak{g}^{(j)}}{du} = u^{\frac{\sigma_j - \mu_j}{\mu_j}} e_1^{(j)}(u).$$

Daraus folgt unter Benutzung von (16) und (17)

$$\left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0 = \sum_{j=1}^{m} \sigma_j - \sum_{j=1}^{m} \mu_j = \left(\mathfrak{G}', \frac{\partial \mathfrak{G}'}{\partial v}\right)_0 - q + 1$$

und wegen (12)

$$\left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0 = (\mathfrak{G}', V)_0 - q + 1. \tag{18}$$

Aus dem Vergleich von (15) und (18) folgt sofort die Behauptung

$$\vartheta_0 = (U, V)_0 = \left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0.$$

III. Wie ϑ von $\langle \mathfrak{G} \rangle$ abhängt.
Beitrag der festen Stellen von $\langle \mathfrak{G} \rangle$.

Wir wollen sehen, welchen Wert $\vartheta_0 = (U, V)_0$ hat, wenn S eine der *festen* Stellen der Kurvenschar $\langle \mathfrak{G} \rangle$ ist.

1. Vorbetrachtung.

Nach (6) ist

$$w - \xi = \frac{\mathfrak{G}}{\mathfrak{G}_a}, \qquad dw = \frac{\mathfrak{G}_a d\mathfrak{G} - \mathfrak{G} d\mathfrak{G}_a}{\mathfrak{G}_a^2} = \mathfrak{X}(U du + V dv),$$

und wegen $\mathfrak{X} = \frac{\mathfrak{T}}{\mathfrak{G}_a^2}$ ist

$$\mathfrak{T}(U du + V dv) = \mathfrak{G}_a^2 dw = \mathfrak{G}_a d\mathfrak{G} - \mathfrak{G} d\mathfrak{G}_a \tag{19}$$

und

$$(20)\qquad \mathfrak{G}_a\frac{\partial\mathfrak{G}}{\partial u}-\mathfrak{G}\frac{\partial\mathfrak{G}_a}{\partial u}=\mathfrak{T}U;\quad \mathfrak{G}_a\frac{\partial\mathfrak{G}}{\partial v}-\mathfrak{G}\frac{\partial\mathfrak{G}_a}{\partial v}=\mathfrak{T}V.$$

Wir setzen

$$(21)\qquad \frac{\partial\mathfrak{G}_a}{\partial u}\frac{\partial\mathfrak{G}}{\partial v}-\frac{\partial\mathfrak{G}}{\partial u}\frac{\partial\mathfrak{G}_a}{\partial v}=\mathfrak{D}\mathfrak{T}$$

und zeigen, daß dieser Ausdruck den Faktor $\mathfrak{T}$ genau in der ersten Potenz enthält, daß also $\mathfrak{D}$ ganz und zu $\mathfrak{T}$ teilerfremd ist.

Es sei $\mathfrak{G}=\mathfrak{P}^\lambda\mathfrak{H}$, wo $\mathfrak{H}$ den Faktor $\mathfrak{P}$ nicht mehr enthält. Es wird für $\mathfrak{P}=0$

$$\frac{1}{\lambda\mathfrak{H}\mathfrak{P}^{\lambda-1}}\left\{\frac{\partial\mathfrak{G}_a}{\partial u}\frac{\partial\mathfrak{G}}{\partial v}-\frac{\partial\mathfrak{G}}{\partial u}\frac{\partial\mathfrak{G}_a}{\partial v}\right\}=\frac{\mathfrak{D}\mathfrak{T}}{\lambda\mathfrak{H}\mathfrak{P}^{\lambda-1}}=\frac{\partial\mathfrak{G}_a}{\partial u}\frac{\partial\mathfrak{P}}{\partial v}-\frac{\partial\mathfrak{G}_a}{\partial u}\frac{\partial\mathfrak{P}}{\partial v}$$

oder, da

$$\frac{\partial\mathfrak{P}}{\partial u}du+\frac{\partial\mathfrak{P}}{\partial v}dv=0\quad\text{für}\quad\mathfrak{P}=0,$$

$$\frac{\mathfrak{D}\mathfrak{T}du}{\lambda\mathfrak{H}\mathfrak{P}^{\lambda-1}}=\frac{\partial\mathfrak{P}}{\partial v}\left\{\frac{\partial\mathfrak{G}_a}{\partial u}du+\frac{\partial\mathfrak{G}_a}{\partial v}dv\right\}=\frac{\partial\mathfrak{P}}{\partial v}d\mathfrak{G}_a.$$

Daraus folgt zunächst, daß $\mathfrak{D}\mathfrak{T}$ mindestens durch $\mathfrak{P}^{\lambda-1}$ teilbar ist. Andrerseits aber auch, daß $\mathfrak{D}\mathfrak{T}$ keine höhere Potenz von $\mathfrak{P}$ enthalten kann; denn sonst müßte $d\mathfrak{G}_a$ für $\mathfrak{P}=0$ verschwinden; dann wäre $\mathfrak{G}_a$ längs $\mathfrak{P}$ konstant, also Null, da $\mathfrak{P}$ und $\mathfrak{G}_a$ in S verschwinden. Es wäre also $\mathfrak{G}_a$ durch $\mathfrak{P}$ teilbar, was nicht möglich ist, weil $\mathfrak{G}_a$ eine Kurve aus $\langle\mathfrak{G}\rangle$ ohne Besonderheiten ist.

2. Formel für $(U,V)_0$.

Nach diesen Vorbereitungen wollen wir den Wert $\vartheta_0=(U,V)_0$ berechnen. Für $V=0$ ist nach (20) und (21)

$$\mathfrak{T}U=-\frac{\mathfrak{G}_a}{\partial\mathfrak{G}_a/\partial v}\cdot\mathfrak{T}\mathfrak{D},$$

also

$$(22)\qquad (U,V)_0=(V,\mathfrak{G}_a)_0-\left(V,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0+(V,\mathfrak{D})_0.$$

Diesen Ausdruck formen wir um:

Für $\mathfrak{G}_a=0$ ist nach (20)

$$(23)\qquad (\mathfrak{G}_a,\mathfrak{G})_0+\left(\mathfrak{G}_a,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0=(\mathfrak{T},\mathfrak{G}_a)_0+(V,\mathfrak{G}_a)_0,$$

und für $\frac{\partial\mathfrak{G}_a}{\partial v}=0$ ist nach (20)

$$\left(\mathfrak{G}_a,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0+\left(\frac{\partial\mathfrak{G}}{\partial v},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0=\left(\mathfrak{T},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0+\left(V,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0$$

und nach (21)

$$\left(\frac{\partial\mathfrak{G}_a}{\partial u},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0+\left(\frac{\partial\mathfrak{G}}{\partial v},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0=\left(\mathfrak{T},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0+\left(\mathfrak{D},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0.$$

Aus der Subtraktion der beiden letzten Gleichungen ergibt sich

$$(24)\qquad \left(\mathfrak{G}_a,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0-\left(\frac{\partial\mathfrak{G}_a}{\partial u},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0=\left(V,\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0-\left(\mathfrak{D},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0.$$

In Verbindung mit (23) und (24) ergibt sich aus (22)

$$(U,V)_0=(\mathfrak{G}_a,\mathfrak{G})_0+\left(\frac{\partial\mathfrak{G}_a}{\partial u},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0-\left(\mathfrak{D},\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0-(\mathfrak{T},\mathfrak{G}_a)_0+(V,\mathfrak{D})_0,$$

also auch

$$(25)\quad (U, V)_0 - \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 - (\mathfrak{G}_a, \mathfrak{G})_0 + (\mathfrak{G}_a, \mathfrak{T})_0 = \left(\mathfrak{D}, \frac{V}{\partial \mathfrak{G}_a/\partial v}\right)_0.$$

Da nun

$$\frac{V}{\partial \mathfrak{G}_a/\partial v} = \frac{U}{\partial \mathfrak{G}_a/\partial u} \quad \text{für} \quad \mathfrak{D} = 0,$$

so ist die linke Seite von (25) auch gleich $U/(\partial \mathfrak{G}_a/\partial u)$, und es folgt nach dem Satz von der korrespondierenden Addition auch

$$(26)\quad (U, V)_0 - \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 - (\mathfrak{G}_a, \mathfrak{G})_0 + (\mathfrak{G}_a, \mathfrak{T})_0 = \left(\mathfrak{D}, \frac{U\,du + V\,dv}{d\mathfrak{G}_a}\right)_0$$
$$= \left(\mathfrak{D}, \frac{\mathfrak{G}_a^2}{\mathfrak{T}}\frac{dw}{d\mathfrak{G}_a}\right)_0 = \left(\mathfrak{D}, \mathfrak{G}_a^2\frac{dw}{d\mathfrak{G}_a}\right)_0 - (\mathfrak{D}, \mathfrak{T})_0.$$

Ist $\mathfrak{D}$ eine Einheit, dann ist die rechte Seite von (26) gleich Null. Für den Fall, daß $\mathfrak{D}$ keine Einheit ist, müssen wir den Ausdruck $(\mathfrak{D}, \mathfrak{G}_a^2\, dw/d\mathfrak{G}_a)_0$ berechnen.

3. Bestimmung von $(\mathfrak{D}, \mathfrak{G}_a^2\, dw/d\mathfrak{G}_a)_0$.

$\mathfrak{D} = 0$ habe die Lösungen

$$v = v_k, \quad (k = 1, 2, \ldots, r),$$

wobei die v_k gewöhnliche Potenzreihen von $u^{\frac{1}{\lambda_k}}$ seien, also

$$v_k = \mathfrak{P}_k(u^{\frac{1}{\lambda_k}}).$$

Für solch' eine Lösung $v = v_k$ mögen $\mathfrak{G}_0(u, v)$ und $\mathfrak{G}_a(u, v)$ übergehen in

$$\mathfrak{G}_0(u, v_k) = \mathfrak{g}_{0k}(u) \quad \text{und} \quad \mathfrak{G}_a(u, v_k) = \mathfrak{g}_{ak}(u) = u^{\frac{\alpha_k}{\lambda_k}} e_{ak}.$$

Wir wählen ξ_k so, daß $\mathfrak{g}_{0k}(u) - \xi_k \mathfrak{g}_{ak}(u)$ durch eine höhere Potenz von u teilbar wird als $\mathfrak{g}_{ak}$. Durch diese Vorschrift ist ξ_k eindeutig bestimmt. Die $\mathfrak{G}_k = \mathfrak{G}_0 - \xi_k \mathfrak{G}_a$ $(k = 1, 2, \ldots, r)$ sind aber nicht notwendig alle verschieden, da die ξ_k zum Teil oder alle einander gleich sein können.

Für $v = v_k$ ist dann

$$\mathfrak{G}_k(u, v_k) = \mathfrak{g}_{kk}(u) = u^{\frac{\beta_k}{\lambda_k}} e_{kk}, \quad \text{und} \quad \beta_k > \alpha_k.$$

Wegen $w = \mathfrak{G}_0/\mathfrak{G}_a$ ist $w - \xi_k = \mathfrak{G}_k/\mathfrak{G}_a$, und es wird

$$(w - \xi_k)_{v=v_k} = \frac{\mathfrak{g}_{kk}}{\mathfrak{g}_{ak}} = u^{\frac{\beta_k - \alpha_k}{\lambda_k}} e_{k1}, \qquad d(w - \xi_k)_{v=v_k} = u^{\frac{\beta_k - \alpha_k - \lambda_k}{\lambda_k}} e_{k2}\, du,$$

$$(\mathfrak{G}_a^2)_{v=v_k} = u^{\frac{2\alpha_k}{\lambda_k}} e_{k3}, \qquad (d\mathfrak{G}_a)_{v=v_k} = d\,\mathfrak{g}_{ak} = u^{\frac{\alpha_k - \lambda_k}{\lambda_k}} e_{k4}\, du,$$

also

$$\left(\frac{dw}{d\mathfrak{G}_a}\,\mathfrak{G}_a^2\right)_{v=v_k} = u^{\frac{\beta_k}{\lambda_k}} e_{k5}.$$

Führen wir nun $u = \tau^{\lambda_k}$ ein, so wird

$$\left(\frac{dw}{d\mathfrak{G}_a}\,\mathfrak{G}_a^2\right)_{v=v_k} = \tau^{\beta_k} e_{k6};$$

es ist also

$$\left(\mathfrak{D}, \frac{dw}{d\mathfrak{G}_a}\,\mathfrak{G}_a^2\right)_0 = \sum_{k=1}^{r} \beta_k.$$

Dies gilt auch, wenn $\mathfrak{D}$ eine Einheit ist, da dann $\mathfrak{D}$ in S keine der Kurven $\mathfrak{G}$ schneidet und daher alle $\beta_k = 0$ zu setzen sind.

Die Gleichung (26) lautet jetzt

$$(27) \quad (U, V)_0 = \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 + (\mathfrak{G}_a, \mathfrak{G})_0 - (\mathfrak{G}_a, \mathfrak{T})_0 - (\mathfrak{D}, \mathfrak{T})_0 + \sum_{k=1}^{r} \beta_k .$$

4. Berechnung von $\Sigma\beta_k$.

Wir betrachten jetzt eine Reihe von Kurven $\mathfrak{H}_l$ ($l = 1, 2, \ldots, \varrho$) der Schar $\langle \mathfrak{G} \rangle$, die folgendermaßen ausgewählt werden sollen:

1. Jede Kurve aus $\langle \mathfrak{G} \rangle$, die einen durch S gehenden mehrfachen Faktor hat, soll unter die $\mathfrak{H}_l$ aufgenommen werden;
2. alle Kurven $\mathfrak{G}_k$ der vorigen Nummer sollen aufgenommen werden, und jede nur einmal.

Der größte gemeinschaftliche Teiler von $\mathfrak{H}_l$ und $\mathfrak{T}$ sei $\mathfrak{T}_l$, wobei nur die durch S gehenden Kurven berücksichtigt zu werden brauchen. Dann ist bei S

$$(28) \qquad d\mathfrak{H}_l = \mathfrak{T}_l(U_l\, du + V_l\, dv),$$

wo U_l und V_l gewöhnliche Potenzreihen von u und v sind. Ferner ist

$$\mathfrak{T} = \prod_{l=1}^{\varrho} \mathfrak{T}_l ,$$

da jeder in $\mathfrak{T}$ enthaltene Primteiler nur in genau *einer* Kurve der Schar $\langle \mathfrak{G} \rangle$ in höherer als der ersten Potenz vorkommt, und da alle die Kurven aus $\langle \mathfrak{G} \rangle$, die einen Primteiler in höherer als der ersten Potenz enthalten, unter die $\mathfrak{H}_l$ aufgenommen sind.

Berücksichtigen wir (28), so wird nach (21)

$$\mathfrak{D}\mathfrak{T} = \mathfrak{T}_l\left(\frac{\partial \mathfrak{G}_a}{\partial u} V_l - \frac{\partial \mathfrak{G}_a}{\partial v} U_l\right);$$

bezeichnen wir den Quotienten $\mathfrak{T}/\mathfrak{T}_l$ mit $\mathfrak{T}^{(l)}$, so wird

$$(29) \qquad \mathfrak{D}\mathfrak{T}^{(l)} = \frac{\partial \mathfrak{G}_a}{\partial u} V_l - \frac{\partial \mathfrak{G}_a}{\partial v} U_l .$$

Für die Schnittpunkte mit $V_l = 0$ folgt daraus

$$(30) \qquad (\mathfrak{D}, V_l)_0 + (\mathfrak{T}^{(l)}, V_l)_0 = \left(\frac{\partial \mathfrak{G}_a}{\partial v}, V_l\right)_0 + (U_l, V_l)_0$$

und für die Schnittpunkte mit $\partial \mathfrak{G}_a/\partial v = 0$

$$(31) \qquad \left(\mathfrak{D}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 + \left(\mathfrak{T}^{(l)}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 = \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 + \left(\frac{\partial \mathfrak{G}_a}{\partial v}, V_l\right)_0 .$$

Entsprechend Jung: Algebraische Flächen S. 320 bezeichnen wir den Beitrag der Kurve $\mathfrak{H}_l$ an der festen Stelle S zu der Zahl δ der Zeuthen-Segreschen Invariante mit

$$\delta_0 = \left(\frac{\partial \mathfrak{H}'}{\partial u}, \frac{\partial \mathfrak{H}'}{\partial v}\right)_0 - \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 .$$

Bedenken wir, daß nach II

$$(U_l, V_l)_0 = \left(\frac{\partial \mathfrak{H}'}{\partial u}, \frac{\partial \mathfrak{H}'}{\partial v}\right)_0 ,$$

so folgt aus der Subtraktion von (30) und (31)

$$\delta_0 = \left(\mathfrak{D}\,\mathfrak{T}^{(l)}, \frac{V_l}{\partial \mathfrak{G}_a/\partial v}\right)_0 ;$$

und da nach (29)

$$\frac{V_l}{\partial \mathfrak{G}_a/\partial v} = \frac{U_l}{\partial \mathfrak{G}_a/\partial u} \quad \text{für} \quad \mathfrak{D}\,\mathfrak{T}^{(l)} = 0\,,$$

so ist ebenfalls

$$\delta_0 = \left(\mathfrak{D}\,\mathfrak{T}^{(l)}, \frac{U_l}{\partial \mathfrak{G}_a/\partial u}\right)_0,$$

und nach dem Satz von der korrespondierenden Addition folgt dann

$$\delta_0 = \left(\mathfrak{D}\,\mathfrak{T}^{(l)}, \frac{U_l du + V_l dv}{d\mathfrak{G}_a}\right)_0$$

und nach (28)

$$\delta_0 = \left(\mathfrak{D}\,\mathfrak{T}^{(l)}, \frac{d\mathfrak{H}_l}{d\mathfrak{G}_a}\right)_0 - (\mathfrak{D}\,\mathfrak{T}^{(l)}, \mathfrak{T}_l)_0\,. \tag{32}$$

Für die Lösung $v = v_k$ von $\mathfrak{D} = 0$ werde wie in Nr. 3

$$\mathfrak{G}_a(u, v_k) = \mathfrak{g}_{ak}(u) = u^{\frac{\alpha_k}{\lambda_k}} e_k\,.$$

Ferner sei

$$\mathfrak{H}_l(u, v_k) = u^{\frac{\gamma_k}{\lambda_k}} e_{lk}\,.$$

Wie wir in Nr. 3 gesehen haben, gehört zu v_k eine ganz bestimmte der Kurven aus $\langle \mathfrak{G} \rangle$, die wieder mit $\mathfrak{G}_k$ bezeichnet sei. Wenn $\mathfrak{H}_l \neq \mathfrak{G}_k$, so ist $\gamma_k = \alpha_k$; wenn $\mathfrak{H}_l = \mathfrak{G}_k$, so ist $\gamma_k = \beta_k$. Es wird

$$(d\mathfrak{H}_l)_{v=v_k} = u^{\frac{\gamma_k - \lambda_k}{\lambda_k}} e_{k1}\,du\,, \qquad (d\mathfrak{G}_a)_{v=v_k} = u^{\frac{\alpha_k - \lambda_k}{\lambda_k}} e_{k2}\,du,$$

$$\left(\frac{d\mathfrak{H}_l}{d\mathfrak{G}_a}\right)_{v=v_k} = u^{\frac{\gamma_k - \alpha_k}{\lambda_k}} e_{k3} = \tau^{\gamma_k - \alpha_k} e_{k4}\,,$$

und für die Zahl der Schnittpunkte folgt

$$\left(\mathfrak{D}, \frac{d\mathfrak{H}_l}{d\mathfrak{G}_a}\right)_0 = \sum_{i=1}^{r} (\gamma_i - \alpha_i)\,, \tag{33}$$

wobei

$$\gamma_k - \alpha_k \begin{cases} = 0 & \text{für} \quad \mathfrak{H}_l \neq \mathfrak{G}_k\,, \\ = \beta_k - \alpha_k & \text{für} \quad \mathfrak{H}_l = \mathfrak{G}_k\,. \end{cases}$$

Ist z. B. $\mathfrak{H}_l$ keiner der Kurven $\mathfrak{G}_k$ gleich, so ist $(\mathfrak{D}, d\mathfrak{H}_l/d\mathfrak{G}_a)_0 = 0$. Ist etwa $\mathfrak{G}_1 = \mathfrak{G}_2 = \mathfrak{G}_3$ und stimmt $\mathfrak{H}_l$ mit diesen Kurven überein, so ist $(\mathfrak{D}, d\mathfrak{H}_l/d\mathfrak{G}_a)_0 = \sum_{i=1}^{3} (\beta_i - \alpha_i)$. Es wird also

$$\sum_{l=1}^{\varrho} \left(\mathfrak{D}, \frac{d\mathfrak{H}_l}{d\mathfrak{G}_a}\right)_0 = \sum_{k=1}^{r} (\beta_k - \alpha_k)\,.$$

Außerdem ist leicht einzusehen, daß

$$\left(\mathfrak{T}^{(l)}, \frac{d\mathfrak{H}_l}{d\mathfrak{G}_a}\right)_0 = 0; \tag{34}$$

denn: es sei $\mathfrak{P}$ ein in $\mathfrak{T}^{(l)}$ enthaltener Primteiler, er sei auch in der Kurve $\mathfrak{G}$ der Schar $\langle \mathfrak{G} \rangle$ enthalten. Diese Kurve $\mathfrak{G}$ kann nicht identisch sein mit $\mathfrak{H}_l$, denn $\mathfrak{H}_l$ enthält keinen Primteiler, der in $\mathfrak{T}^{(l)}$ vorkommt. Betrachten wir als Grundkurven der Schar $\langle \mathfrak{G} \rangle$ die Kurven $\mathfrak{H}_l$ und $\mathfrak{G}_a$, so läßt sich $\mathfrak{G}$ darstellen in der Form

$$\mathfrak{G} = \mathfrak{H}_l + \alpha \mathfrak{G}_a\,,$$

wo $\alpha \neq 0$ ist. Aus der Differentiation dieser Gleichung folgt für $\mathfrak{P} = 0$ (da damit auch $\mathfrak{G} = 0$ und $d\mathfrak{G} = 0$)

$$d\mathfrak{H}_l = -\alpha\, d\mathfrak{G}_a .$$

Der Quotient $d\mathfrak{H}_l/d\mathfrak{G}_a$ ist also für $\mathfrak{T}^{(l)} = 0$ eine Konstante, woraus (34) folgt.

Nach (33) und (34) lautet jetzt (32)

$$\delta_0 = \sum_{l=1}^{\varrho} \delta_{0l} = \sum_{k=1}^{r} (\beta_k - \alpha_k) - \sum_{l=1}^{\varrho} (\mathfrak{D}\mathfrak{T}^{(l)}, \mathfrak{T}_l)_0 \tag{35}$$

$$= \sum_{k=1}^{r} \beta_k - \sum_{k=1}^{r} \alpha_k - (\mathfrak{D}, \mathfrak{T})_0 - \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l)_0 .$$

5. Berechnung von $\Sigma\alpha_k$.

Es habe $\mathfrak{G}_a = 0$ die Lösungen

$$v = v^{(k)}, \quad (k = 1, 2, \ldots, s),$$

wobei die $v^{(k)}$ von der Form sind

$$v^{(k)} = \mathfrak{P}_k\left(u^{\frac{1}{\mu_k}}\right).$$

Mit $\mathfrak{G}_a = 0$ ist auch $d\mathfrak{G}_a = (\partial\mathfrak{G}_a/\partial u)\, du + (\partial\mathfrak{G}_a/\partial v) dv = 0$, und für $v = v^{(k)}$ ist damit

$$(\mathfrak{D}\mathfrak{T})_{v=v^{(k)}} = \left(\frac{\partial\mathfrak{G}_a}{\partial u}\frac{\partial\mathfrak{G}}{\partial v} - \frac{\partial\mathfrak{G}_a}{\partial v}\frac{\partial\mathfrak{G}}{\partial u}\right)_{v=v^{(k)}} \tag{36}$$

$$= -\frac{1}{du}\frac{\partial\mathfrak{G}_a}{\partial v}\left\{\frac{\partial\mathfrak{G}}{\partial v} dv + \frac{\partial\mathfrak{G}}{\partial u} du\right\} = -\frac{1}{du}\frac{\partial\mathfrak{G}_a}{\partial v} d\mathfrak{G},$$

wo $\mathfrak{G}$ jetzt eine, von $\mathfrak{G}_a$ verschiedene, fest gewählte Kurve des Büschels sein soll. Nun sei für $v = v^{(k)}$

$$\mathfrak{G}(u, v^{(k)}) = u^{\frac{\delta_k}{\mu_k}} e_{k6} = \tau^{\delta_k} e_{k7} ,$$

also

$$(\mathfrak{G}, \mathfrak{G}_a)_0 = \sum_{k=1}^{s} \delta_k ;$$

und

$$d\mathfrak{G}(u, v^{(k)}) = u^{\frac{\delta_k - \mu_k}{\mu_k}} e_{k8} du = \tau^{\delta_k - 1} e_{k9} d\tau ,$$

also

$$(d\mathfrak{G}, \mathfrak{G}_a)_0 = \sum_{k=1}^{s} (\delta_k - 1) . \tag{37}$$

Da $(\mathfrak{D}, \mathfrak{G}_a)_0 = \sum_{k=1}^{r} \alpha_k$ ist, so wird

$$(\mathfrak{D}\mathfrak{T}, \mathfrak{G}_a)_0 = (\mathfrak{T}, \mathfrak{G}_a)_0 + \sum_{k=1}^{r} \alpha_k ,$$

oder wenn wir wie üblich den Beitrag der Stelle S zur Ordnung des Divisors der mehrfachen Stellen von $\mathfrak{G}_a$ mit

$$\left(\mathfrak{G}_a, \frac{1}{du}\frac{\partial\mathfrak{G}_a}{\partial v}\right)_0 = 2\,\sigma_{a0}$$

bezeichnen, so wird andrerseits nach (36) und (37)

$$(\mathfrak{D}\,\mathfrak{T}, \mathfrak{G}_a)_0 = \sum_{k=1}^{s} (\delta_k - 1) + 2\sigma_{a0} = (\mathfrak{G}_a, \mathfrak{G})_0 + 2\sigma_{a0} - \nu_{a0} ,$$

wobei $\nu_{a0} = s$ die Zahl der Zweige einer allgemeinen Kurve $\mathfrak{G}_a$ ist, die durch S gehen. Es ist also

$$\sum_{k=1}^{r} \alpha_k = (\mathfrak{G}_a, \mathfrak{G})_0 + 2\sigma_{a0} - \nu_{a0} - (\mathfrak{T}, \mathfrak{G}_a)_0 ,$$

und damit ist nach (35)

$$\sum_{k=1}^{r} \beta_k = \delta_0 + (\mathfrak{G}_a, \mathfrak{G})_0 + 2\sigma_{a0} - \nu_{a0} - (\mathfrak{T}, \mathfrak{G}_a)_0 + (\mathfrak{D}, \mathfrak{T})_0 + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l)_0 .$$

Außerdem ist nach Jung: Algebraische Flächen S. 319

$$\left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 = 2\sigma_{a0} - \nu_{a0} + 1 .$$

Setzen wir die jetzt gefundenen Resultate in (27) ein, so wird die gesuchte Zahl der Schnittpunkte

$$(38) \quad (U, V)_0 = \delta_0 + 4\sigma_{a0} - 2\nu_{a0} + 1 + 2\,(\mathfrak{G}_a, \mathfrak{G})_0 - 2\,(\mathfrak{T}, \mathfrak{G}_a)_0 + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l)_0 .$$

Summieren wir jetzt über alle festen Stellen der Kurvenschar $\langle \mathfrak{G} \rangle$, so wird $\Sigma(\mathfrak{G}_a, \mathfrak{G})_0 = (\mathfrak{G}_a, \mathfrak{G})$, da die Kurven des Büschels sich nur in den festen Stellen treffen. Ferner ist $(\mathfrak{G}_a, \mathfrak{G}) = (\mathfrak{G}_a, \mathfrak{G}_a)$, da $\mathfrak{G}_a \sim \mathfrak{G}$ ist. Aus (38) folgt daher

$$\sum_S (U, V)_0 = \sum_S \delta_0 + 4\sigma_a - 2\nu_a + f + 2\,(\mathfrak{G}_a, \mathfrak{G}_a) - 2\,(\mathfrak{T}, \mathfrak{G}_a) + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l) .$$

Für die nicht festen Stellen war nach II

$$\sum_S (U, V)_0 = \sum_S \left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0 = \sum_S \delta_0 ,$$

worin die Summe über alle nicht festen Stellen zu erstrecken ist. Berücksichtigen wir jetzt *sämtliche* Stellen des betrachteten algebraischen Körpers, so folgt, wenn wir

$$\sum_S \delta_0 = \delta'$$

setzen,

$$(39) \quad \sum_S (U, V)_0 = \vartheta = \delta' + 4\sigma_a - 2\nu_a + f + 2(\mathfrak{G}_a, \mathfrak{G}_a) - 2(\mathfrak{T}, \mathfrak{G}_a) + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l) ,$$

wo S sämtliche Stellen durchläuft.

IV. Definition der Zeuthen-Segreschen Invariante.

Wir setzen nun die gefundenen Ausdrücke in die Invariante

$$(5) \qquad I = \vartheta + (\mathfrak{X}, \mathfrak{K}) - (\mathfrak{X}, \mathfrak{X})$$

ein, um sie durch Größen auszudrücken, die sich auf die Kurvenschar $\langle \mathfrak{G} \rangle$ beziehen. Nach (7) und (39) wird dann

$$I = \delta' + 4\sigma_a - 2\nu_a + f + 2(\mathfrak{G}_a, \mathfrak{G}_a) - 2(\mathfrak{G}_a, \mathfrak{T}) + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l) + \left(\frac{\mathfrak{T}}{\mathfrak{G}_a}, \mathfrak{K}\right) - \left(\frac{\mathfrak{T}}{\mathfrak{G}_a^2}, \frac{\mathfrak{T}}{\mathfrak{G}_a^2}\right) .$$

Anders geordnet ist

$$I = \delta' - 2\,\{(\mathfrak{G}_a, \mathfrak{G}_a \mathfrak{K}) - 2\sigma_a\} - (2\nu_a - f) + 2(\mathfrak{G}_a, \mathfrak{T}) + (\mathfrak{K}, \mathfrak{T}) + \sum_{l=1}^{\varrho} (\mathfrak{T}^{(l)}, \mathfrak{T}_l) - (\mathfrak{T}, \mathfrak{T}) .$$

Es ist aber

$$(\mathfrak{G}_a, \mathfrak{G}_a \mathfrak{K}) - 2\sigma_a = 2\pi - 2 .$$

Ferner setzen wir

$$2\nu_a - f = N .$$

Dann ist

$$I = \delta' - 4(\pi - 1) - N + \tau ,$$

wobei gesetzt ist

$$\tau = 2(\mathfrak{G}_a, \mathfrak{T}) + (\mathfrak{T}, \mathfrak{K}) + \sum_{\lambda=1}^{\varrho} \left(\frac{\mathfrak{T}}{\mathfrak{T}_l}, \mathfrak{T}_l\right) - (\mathfrak{T}, \mathfrak{T}) .$$

Wegen $\mathfrak{T} = \prod_{l=1}^{\varrho} \mathfrak{T}_l$ ist auch

$$\tau = 2(\mathfrak{G}_a, \mathfrak{T}) + (\mathfrak{T}, \mathfrak{K}) - \sum_{l=1}^{\varrho} (\mathfrak{T}_l, \mathfrak{T}_l).$$

Setzen wir noch

$$\delta' + \tau = \delta,$$

so erhalten wir für die Invariante I die Form

$$I = \delta - 4\pi - N + 4.$$

Die Bedeutung von δ' sei nochmals angegeben:

Ist S nicht eine der festen Stellen von $\langle \mathfrak{G} \rangle$ und $\mathfrak{G}$ die durch S gehende Kurve der Schar, so ist der Beitrag, den S zu δ' liefert

$$\delta_0 = \left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0,$$

wo $\mathfrak{G}'$ dieselben Primteiler enthält wie $\mathfrak{G}$, aber jeden genau in der ersten Potenz.

Ist S eine feste Stelle von $\langle \mathfrak{G} \rangle$, so ist der Beitrag von S zu δ'

$$\delta_0 = \sum_{\mathfrak{G}} \left\{ \left(\frac{\partial \mathfrak{G}'}{\partial u}, \frac{\partial \mathfrak{G}'}{\partial v}\right)_0 - \left(\frac{\partial \mathfrak{G}_a}{\partial u}, \frac{\partial \mathfrak{G}_a}{\partial v}\right)_0 \right\}.$$

Dann ist

$$\delta' = \sum_{S} \delta_0,$$

wo über alle Stellen S von F zu summieren ist.

Betrachten wir den einfachen Fall:

1. keine der Kurven $\mathfrak{G}$ hat mehrfache Faktoren,
2. die Kurven aus $\langle \mathfrak{G} \rangle$ haben höchstens Doppelpunkte mit getrennten Tangenten,
3. durch die festen Stellen gehen die Kurven nur einfach.

Dann gilt:

1. $\mathfrak{T} = 1$, also $\tau = 0$ und $\delta' = \delta$,
2. $\nu_a = f$, also $N = 2\nu_a - f = f$,
3. ist S eine feste Stelle, so ist $\delta_0 = 0$ wegen $\mathfrak{G} = \mathfrak{G}'$; ist S keine der festen Stellen und hat die Kurve $\mathfrak{G}$, die durch S geht, in S einen Doppelpunkt, so ist $\delta_0 = 1$, sonst ist auch hier $\delta_0 = 0$. $\delta_0 = \delta' = \delta$ wird also gleich der Anzahl der Kurven mit Doppelpunkt.

In diesem einfachen Falle wird also

$$I = Z + 4, \tag{40}$$

wenn wir die Zeuthen-Segresche Invariante wie in (1) definieren. Da I nach dem in der Einleitung angeführten Beweis invariant ist, so folgt dasselbe für Z, wenn wir Z durch (40) definieren.

Damit haben wir einmal eine in allen Fällen gültige Definition von Z gegeben und gleichzeitig die Invarianz von Z bewiesen.

Literaturverzeichnis.

Heinrich W. E. Jung: Über die Zeuthen-Segresche Invariante, Rendiconti del Circolo matematico di Palermo, Bd. XXXIV, S. 225—277.

Heinrich W. E. Jung: Algebraische Flächen. Kap. VI.

Francesco Severi: La serie canonica e la teoria delle serie principali di gruppi di punti sopra una superficie algebrica. Commentarii Mathematici Helvetici, Bd. 4, MCMXXXII.

Heinrich W. E. Jung: Sui gruppi di punti sopra una superficie e sulla serie di Severi, dal punto di vista della teoria dei corpi algebrici. Reale Acc. d'Italia. Memorie della classe di sc. fis. mat. e nat. Bd. IV, S. 403—413.

Eingegangen 5. September 1933.

Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper[1]).

Von *L. Rédei* in Mezötur (Ungarn).

Der hier arithmetisch zu beweisende Satz ist bisher nur funktionentheoretisch, nämlich mit der Hilfe der Klassenkörpertheorie begründet [2]) [3]).

Durchgängige Zeichen:

k ein beliebiger quadratischer Zahlkörper;

D die Diskriminante von k;

$p_1, p_2, \ldots, p_t$ sämtliche verschiedene rationale Primteiler von D, t deren Anzahl; ist D gerade, so ist $p_t = 2$; ist p_i ungerade, so ist $p_i \equiv 1 \pmod 4$ — letztere p_i sind also mit geeignetem Vorzeichen versehen; ich setze $t \geqq 2$ voraus, da der Fall $t = 1$ trivial ist;

P ist das Produkt einiger verschiedener p_i oder $P = 1$;

Q ist das Produkt einiger verschiedener $| p_i |$ oder $Q = 1$;

$[a]$ (der quadratfreie Kern von a) erklärt für rationale $a(\neq 0)$ durch: $[a]$ ganz rational, frei von ganz-rationalen Quadratzahlfaktoren; $[a] = ab^2$, b rational;

$P' = [PD]$, $Q' = [QD]$;

a Res b ist das Zeichen für die Lösbarkeit von $a \equiv x^2 \pmod b$(a, b, x ganz rational, $b \neq 0$);

$(\frac{\cdot\cdot}{\cdot\cdot})$ ist das Symbol von Legendre-Jacobi-Kronecker;

$(\ldots, \ldots)$ ist das Zeichen für den größten gemeinsamen Teiler (Ideal);

N ist das Zeichen für die Norm in k;

$\mathfrak{Q}$ ist das Ideal in k mit $\mathfrak{Q}^2 = Q$; es ist also $N(\mathfrak{Q}) = Q$.

1. Es bedeute H die Gruppe der durch total-positive Zahlen von k erzeugbaren Hauptideale. Die bei der Einteilung aller (ganzen und gebrochenen) Ideale von k nach H entstandenen Klassen mögen als absolute Idealklassen bezeichnet werden. Diese bilden die abelsche Gruppe $\mathfrak{H}$ (d. h. die in „engerem“ Sinne genommene absolute Klassengruppe von k). Es bezeichne e_4 die Anzahl der durch vier teilbaren Invarianten von $\mathfrak{H}$. *Die beiligende Arbeit beschäftigt sich mit der Bestimmung von* e_4.

[1]) Der hier mitzuteilende Aufsatz wird auch ungarisch erscheinen als: Rédei, A másodfoku számtest egyik tételének uj bizonyitása, Math. u. Naturwiss. Anz. d. ung. Ak. **50** (1933).

[2]) L. Rédei u. H. Reichardt: Die durch vier teilbaren Invarianten der Klassengruppe des quadratischen Zahlkörpers, Journ. f. d. Math. **170** (1933), S. 69—74; im folgenden zitiert mit RR.

H. Reichardt: Zur Struktur der absoluten Idealklassengruppe im quadratischen Zahlkörper, ebenda, S. 75—82. Diese Arbeiten werden hier nicht vorausgesetzt.

[3]) Es möge hier auch nicht unerwähnt bleiben, daß vor kurzem ein Teil der Dirichletschen Klassenzahlformeln auch eine arithmetische Tatsache geworden ist in der Arbeit von B. A. Wenkov, Über die Klassenzahl positiver binärer quadratischer Formen, Math. Zeitschr. **33** (1931), S. 350—374.

Nach dem Hauptsatze der Theorie der abelschen Gruppen gilt:

2. 2^{e_4} *ist gleich der Anzahl sämtlicher verschiedenen Idealklassen* C^2 *mit* $C^4 = H$.

Andererseits besteht für diese C^2 die Gleichung $(C^2)^2 = H$, sie kommen also in den Idealklassen B mit $B^2 = H$ („ambige" Klassen) vor. Letztere B sind alle durch die Ideale $\mathfrak{Q}$ repräsentiert, und zwar enthält jedes B genau zwei $\mathfrak{Q}$ [4]). Dann ist also

$$2^{e_4} = \tfrac{1}{2}\, n, \tag{1}$$

wobei n die Anzahl derjenigen verschiedenen $\mathfrak{Q}$ bedeutet, für welche

$$\mathfrak{a}^2 = (\alpha)\,\mathfrak{Q} \tag{2}$$

befriedigt werden kann; dabei ist $\mathfrak{a}$ ein ganzes Ideal in k, α eine total-positive Zahl in k. Nach einem elementaren Satze kann auch $(\mathfrak{a}, D) = 1$ vorausgesetzt werden (jede Idealklasse enthält ganze Ideale, die zu einem vorgegebenen Ideal relativ prim sind).

Ich behaupte, daß

3. (2) *und*

$$u^2Q - v^2Q' - w^2 = 0 \tag{3}$$

gleichzeitig lösbar oder unlösbar sind; eine Lösung von (3) ist immer in rationalen u, v, w zu verstehen, die alle von Null verschieden sind.

Besteht nämlich (2) und ist $\alpha = x + y\sqrt{D}$ mit $N(\alpha) = x^2 - y^2 D > 0$, so ist

$$N(\mathfrak{a})^2 = (x^2 - y^2 D)\,Q,$$

und somit ist (3) lösbar, da $[DQ] = Q'$.

Umgekehrt, wenn (3) lösbar ist, dann können zunächst u, v, w positiv ganz und paarweise relativ prim vorausgesetzt werden. Dann sind auch die Glieder der linken Seite von (3) paarweise relativ prim, oder sie haben paarweise 2 als größten gemeinsamen Teiler, letzteres dann und nur dann, wenn $Q \equiv Q' \equiv 0 \pmod 2$. Ich betrachte dann das Ideal

$$\mathfrak{a} = (w,\, uQ + v\sqrt{QQ'});$$

dies ist ein ganzes Ideal in k, da $[QQ'] = [Q^2 D] = [D]$. Nach Quadrieren ergibt sich

$$\mathfrak{a}^2 = (w^2,\, (uQ + v\sqrt{QQ'})^2).$$

Mit der Umformung $(a, b) = (a, b + Qa)$ folgt nach (3):

$$\mathfrak{a}^2 = (w^2,\, 2uQ(uQ + v\sqrt{QQ'})).$$

Hier läßt sich aus dem Faktor $2uQ$ wegen $(u, w) = 1$ zunächst u und leicht ersichtlich [5]) auch Q streichen. Multipliziert man dann mit Q und berücksichtigt (3), so folgt

$$Q\,\mathfrak{a}^2 = (uQ + v\sqrt{QQ'})\,(uQ - v\sqrt{QQ'},\, 2Q).$$

Der zweite Faktor der rechten Seite ist $\mathfrak{Q}$ oder $2\mathfrak{Q}$ [6]), der erste Faktor ist Hauptideal in k, und somit besteht (2) und die Behauptung **3.**

4. Nach *Lagrange* [7]) ist für die Lösbarkeit von (3) notwendig und hinreichend, daß

---

[4]) S. z. B. Hecke, Vorl. über alg. Zahlen (1923), S. 179—181.

[5]) Das ist selbstverständlich im Falle $(Q, w) = 1$. Ist $(Q, w) = 2$, so sind u, v ungerade, Q' gerade nach (3), es ist also $D \equiv -4 \pmod{16}$, $\frac{Q}{2}\frac{Q'}{2} \equiv -1 \pmod 4$; dann ist $w^2 \equiv 4 \pmod 8$ nach (3); da nun $4 \mid 2(uQ + v\sqrt{QQ'})$, so zieht das obige Streichen von Q nicht das Auslassen eines Idealfaktors mit sich. Der Fall $(Q, w) > 2$ kann nicht vorkommen, da dann nach der Definition Q und w einen ungeraden Primzahlteiler gemeinsam hätten, der dann nach (3) auch in v enthalten wäre.

[6]) Eine „Abweichung" kann sich nämlich nur in den Primidealfaktoren von 2 zeigen. Es reicht also aus, den Fall „$N(uQ - v\sqrt{QQ'}) = w^2Q$ gerade" zu diskutieren, und dann ergibt sich leicht die Richtigkeit der obigen Behauptung.

[7]) S. z. B. Dirichlet-Dedekind, Zahlentheorie, 4. Aufl. (1894), S. 432.

(4) $$Q \text{ Res } Q', \quad -Q' \text{ Res } Q.$$ [8] [9] [10]

5. Ich führe die Matrix

(5) $$M_D = \begin{pmatrix} \left(\frac{D}{p_1}\right) & \left(\frac{p_2}{p_1}\right) & \left(\frac{p_3}{p_1}\right) & \cdots & \left(\frac{p_{t-1}}{p_1}\right) \\ \left(\frac{p_1}{p_2}\right) & \left(\frac{D}{p_2}\right) & \left(\frac{p_3}{p_2}\right) & & \left(\frac{p_{t-1}}{p_2}\right) \\ \left(\frac{p_1}{p_3}\right) & \left(\frac{p_2}{p_3}\right) & \left(\frac{D}{p_3}\right) & & \left(\frac{p_{t-1}}{p_3}\right) \\ \vdots & & & & \\ \left(\frac{p_1}{p_{t-1}}\right) & \left(\frac{p_2}{p_{t-1}}\right) & \left(\frac{p_3}{p_{t-1}}\right) & & \left(\frac{D}{p_{t-1}}\right) \\ \left(\frac{p_1}{p_t}\right) & \left(\frac{p_2}{p_t}\right) & \left(\frac{p_3}{p_t}\right) & & \left(\frac{p_{t-1}}{p_t}\right) \end{pmatrix}$$

ein, in welcher also die Anzahl der Zeilen bzw. Spalten gleich t bzw. $t-1$ ist und jedes Element gleich ± 1. Die i-te Zeile (Spalte) wird auch als „die zu p_i gehörige Zeile (Spalte)" bezeichnet werden. Allgemeiner bedeuten „die zu P gehörigen Zeilen (Spalten) von M_D" die Menge der zu den Primzahlfaktoren von P gehörigen Zeilen (Spalten); darunter möge die leere Menge verstanden werden, wenn $P = 1$ ist.

Ich nehme einige Zeilen $a, b, \ldots, m$ einer beliebigen Matrix und multipliziere der Reihe nach immer die in derselben Spalte enthaltenen Elemente miteinander. Das System der so erhaltenen Zahlen nenne ich das Produkt $ab \cdots m$; der leeren Menge der Zeilen ordne ich die Zahlen $1, 1, \ldots, 1$ (so viel Einsen wie die Anzahl der Spalten) als Produkt zu. Es ist das Produkt von Spalten ähnlich zu verstehen.

---

[8]) Obiges folgt unmittelbar nur im Falle $(Q, Q') = 1$. In anderem Falle muß $(Q, Q') = 2$ sein; dann ist w gerade und (3) geht in $u^2 \cdot \frac{Q}{2} - v^2 \cdot \frac{Q'}{2} - \left(\frac{w}{2}\right)^2 \cdot 2 = 0$ über, wobei die Koeffizienten $\frac{Q}{2}, \frac{-Q'}{2}, -2$ paarweise teilerfremd sind. Somit folgt nach [7]) Q Res $\frac{Q'}{2}, -Q'$ Res $\frac{Q}{2}, \frac{Q}{2} \cdot \frac{Q'}{2}$ Res 2 als notwendiges und hinreichendes Kriterium für die Lösbarkeit von (3). Die Abweichung von (4) ist nur formal, da a Res 2, wenn a ganz rational ist.

[9]) Nach (1), **3.** und **4.** ist also 2^{e_4} die Hälfte der Anzahl der Zahlenpaare Q, Q', die (4) befriedigen. Damit ist zwar e_4 vollständig bestimmt, ich betrachte dies aber nur als ein vorläufiges Resultat, nicht nur darum, weil die Bestimmungsart von e_4 durch die aus den Arbeiten[2]) bekannten und im folgenden auch hier einzuführenden „D-Zerfällungen zweiter Art" auch formal einfacher wird, sondern auch darum, weil (nach den erwähnten Arbeiten) die „D-Zerfällungen" und gewisse absolute Klassenkörper über k eng miteinander zusammenhängen. (Ein ähnlicher direkter Zusammenhang läßt sich über die Zahlenpaare Q, Q' nicht aussagen.) — Zwar sind die (4) befriedigenden Zahlenpaare Q, Q' und D-Zerfällungen zweiter Art nur wenig voneinander abweichende Begriffe, doch lassen sie sich ineinander nur auf einem ziemlich künstlichen Wege überführen. Dies leistet die oben gleich zu definierende Matrix.

[10]) Nach dem in [9]) anfangs Gesagten gibt es stets wenigstens zwei Lösungen Q, Q' von (4). Eine erste (triviale) Lösung ist 1, $[D]$. Eine zweite ist: 1.) $|[D]|, -1$, wenn $D < 0$; 2.) $[D], 1$, wenn $D > 0$ und die positiven ungeraden Primzahlfaktoren von D alle von der Gestalt $4e + 1$ sind; ist weiter $D > 0$ und $N(\varepsilon) = 1$, wo ε eine Grundeinheit in k ist — und dies ist stets der Fall, wenn 3.) $D > 0$ und nicht unter 2.) gehört — so ist nach Dirichlet aus ε eine Lösung $Q_\varepsilon, Q'_\varepsilon$ von (4) ableitbar, für welche $|Q_\varepsilon| \neq 1$, $|Q'_\varepsilon| \neq 1$ ist (vgl. z. B. das Ende von RR); selbst im Falle 2.) und nur in ihm ist dann auch $Q'_\varepsilon, Q_\varepsilon$ eine Lösung von (4). — Schon hier läßt sich also nach [9]) die Folgerung ziehen: Im Falle 2.) ist $N(\varepsilon) = -1$, wenn $e_4 = 0$ (vgl. das Ende von RR).

Ich spreche von einer *Einheitsmenge* von Zeilen (Spalten) einer Matrix, wenn das zugehörige Produkt $1, 1, \ldots, 1$ ist. Die leere Menge der Zeilen (Spalten) ist stets eine Einheitsmenge.

Ich beweise folgendes:

6. *Die Menge der zu P gehörigen Zeilen von M_D ist dann und nur dann eine Einheitsmenge, wenn $Q = |P|$ (4) befriedigt.*

Zunächst betrachte ich das Produkt der zu P gehörigen Zeilen von M_D. Es ist nach (5)

$$\left(\frac{p'}{P}\right), \quad \left(\frac{p}{\frac{P}{p}}\right)\cdot\left(\frac{\frac{D}{p}}{p}\right) \qquad (p \mid P,\ p' \mid P';\ \ p, p' \neq p_t), \tag{6}$$

wobei p und p' diejenige Primzahlen aus $p_1, p_2, \ldots, p_{t-1}$ bedeuten, die in P bzw. P' enthalten sind (es ist ja $(P, P') = 1$ oder p_t, letzteres nur bei geradem D); (6) ist auch für $p = 1$ das richtige Produkt, da dann $\left(\frac{p'}{1}\right) = 1$ und p nicht vorhanden ist. Nach dem quadratischen Reziprozitätsgesetz geht (6) in

$$\left(\frac{P}{p'}\right)\left(\frac{-1}{p'}\right)^{\frac{\operatorname{Sgn} P-1}{2}}, \quad \left(\frac{P'}{p}\right)\left(\frac{-1}{p}\right)^{\frac{\operatorname{Sgn} P+1}{2}}, \qquad (p, p' \text{ wie oben}) \tag{7}$$

über, wobei auch $\left[\frac{P}{p}\cdot\frac{D}{p}\right] = P'$ berücksichtigt ist (Sgn a für $a \neq 0$ erklärt durch $a = \operatorname{Sgn} a \cdot |a|$).

Andererseits läßt sich (4) durch

$$Q \text{ Res } Q'_*, \quad -Q' \text{ Res } Q_* \tag{4'}$$

ersetzen, wobei „*“ das Streichen des zufälligen Faktors p_t bedeutet, d. h. z. B. $Q_* = Q$, wenn $p_t \nmid Q$, und $p_t Q_* = Q$, wenn $p_t \mid Q$.

Ist nämlich $p_t = 2$, so unterscheiden sich (4) und (4') nur formal voneinander, da a Res 2 für jedes ganz rationale a besteht. Ist aber p_t und somit D ungerade, so geht (4) in

$$\left(\frac{Q}{q'}\right) = 1, \quad \left(\frac{-Q'}{q}\right) = 1 \tag{8}$$

über, wobei q und q' sämtliche Primzahlfaktoren von Q bzw. Q' bedeuten. Das Produkt der linken Seiten in (8) ist

$$\left(\frac{Q}{Q'}\right)\left(\frac{-Q'}{Q}\right),$$

und das ist nach dem Reziprozitätsgesetz gleich 1, da $Q > 0$ und jetzt $QQ' = D \equiv 1 \pmod 4$. Dann ist also jede Gleichung von (8) eine Folge der übrigen, und wenn man dies im besonderen für die Gleichung berücksichtigt, in welcher der „Nenner“ p_t vorkommt, so ergibt sich die Richtigkeit der Behauptung über (4').

Zum Beweise von **6.** reicht es also aus, zu zeigen, daß die Zahlen von (7) dann und nur dann gleich 1 sind, wenn (4') für $Q = |P|$ besteht. Letzteres folgt aber unmittelbar aus der Bemerkung, daß die Zahlen von (7) je nach den Fällen $P > 0$, $P < 0$ in

$$\left(\frac{P}{p'}\right), \quad \left(\frac{-P'}{p}\right) \text{ bzw. } \left(\frac{-P}{p'}\right), \quad \left(\frac{P'}{p}\right)$$

übergehen (bei $Q = eP$, $e = \pm 1$ ist ja $Q' = eP'$).

Ich beweise den *Hilfssatz*:

7. *Ist eine r-zeilige und s-spaltige Matrix aus Elementen* ± 1 *gegeben, und sind* R *und* S *die Anzahl der Einheitsmengen der Zeilen bzw. Spalten, so ist* $\frac{R}{S} = 2^{r-s}$ [11]).

Vor allem sieht man ein, daß R und S unverändert bleiben, wenn a durch $a' = ab$ ersetzt wird, wobei a, b zwei verschiedene Zeilen der Matrix bedeuten. Es sei nämlich h eine Einheitsmenge von Zeilen. Enthält h a nicht, so gehört h auch der neuen Matrix an (und ist auch in dieser eine Einheitsmenge). Enthält h a, so streicht man b aus h oder nimmt b hinzu, je nachdem h b enthält oder nicht, und ersetzt man noch a durch $a' = ab$; so entsteht offenbar eine Einheitsmenge der Zeilen der neuen Matrix. Damit habe ich auch in der neuen Matrix R verschiedene Einheitsmengen von Zeilen aufgezählt, und somit wird R bei der Operation „a' statt a" nicht verkleinert. Dann muß sogar R unverändert bleiben, denn die nochmalige Operation „$a'b = ab^2 = a$ statt a'" führt zur alten Matrix zurück. — Das Unverändertbleiben von S bei „a' statt a" ergibt sich sofort daraus, daß, wenn $A, B, C, \ldots$ das Produkt einiger Spalten der alten Matrix ist, wobei A und B das Produkt der in der Zeile a bzw. b enthaltenen Elemente der gegebenen Spalten ist, dann das Produkt der entsprechenden Spalten in der neuen Matrix $AB, B, C, \ldots$ ist, und dies besteht aus lauter Einsen dann und nur dann, wenn Entsprechendes auch für $A, B, C, \ldots$ gilt.

Ebenso bleiben R, S auch dann ungeändert, wenn eine Spalte mit einer anderen Spalte multipliziert wird.

Nunmehr ist **7.** richtig, wenn die Matrix aus lauter 1 besteht, da dann jede Menge von Zeilen und Spalten eine Einheitsmenge ist, und somit $R = 2^r$, $S = 2^s$ ist. **7.** ist auch dann richtig, wenn $s = 1$ und die Matrix nicht aus lauter Einsen besteht, da dann $R = 2^{r-1}$, $S = 1$. Im folgenden läßt sich also **7.** für die kleineren Werte von s und zugleich das erste Element der Matrix als -1 voraussetzen. Multipliziert man mit der ersten Zeile geeignete andere Zeilen nacheinander, und verfährt ähnlich mit den Spalten, so lassen sich die Elemente der ersten Zeile und Spalte in 1 umwandeln, nur das (einzige) gemeinsame Element behält seinen Wert -1 bei. Diese Operationen lassen R und S unverändert. Letztere verändern sich auch dann nicht, wenn noch die erste Zeile und Spalte gestrichen wird, da diese nicht mehr in den Einheitsmengen (von Zeilen oder Spalten) vorkommen können. Nach der Voraussetzung ist also $\frac{R}{S} = 2^{(r-1)-(s-1)} = 2^{r-s}$ und somit ist **7.** allgemein richtig.

8. *Zusammenfassung des Bisherigen*: Das n in (1) — welches erst die Anzahl der $\mathfrak{Q}$ bedeutete, die (2) erfüllen — ist die Anzahl der Q, für die (3) lösbar ist, d. h. die (4) befriedigen. Weiter ist n nach **6.** gleich der Anzahl der Einheitsmengen von Zeilen von M_D, d. h. nach **7.** gleich $2n_1$, wobei n_1 *die Anzahl der Einheitsmengen von Spalten von* M_D *bedeutet*, und zugleich nach (1):

$$2^{e_4} = n_1. \tag{9}$$

Für die nähere Bestimmung von n_1 betrachte ich das Produkt der zu P gehörigen Spalten von M_D:

$$\left(\frac{P}{p'}\right), \quad \left(\frac{\frac{P}{p}}{p}\right) \cdot \left(\frac{\frac{D}{p}}{p}\right) = \left(\frac{P'}{p}\right) \qquad (p_t \mid P;\ p \mid P,\ p' \mid 2P'), \tag{10}$$

[11]) Schreibt man die Elemente a_{ik} der obigen Matrix in der Form $(-1)^{e_{ik}} (e_{ik} = 0, 1)$, so läßt sich die Behauptung in eine über die Matrix (e_{ik}) übersetzen und dann leicht mit Hilfe der allgemeinen Theorie der Matrizen im Restklassenkörper nach 2 bestätigen (s. z. B. Hasse, Höhere Algebra I, Berlin u. Leipzig (1933), S. 97, Satz 53), doch gebe ich hier aus methodischen Gründen einen kurzen Beweis an.

wobei P der Einschränkung $p_t \mid P$ unterworfen ist und p, p' diejenigen Primzahlen aus $p_1, p_2, \ldots, p_t$ bedeuten, die in P bzw. $2P'$ enthalten sind. (Es ist zu bemerken, daß hier P ungerade ist und somit $(P, 2P') = 1$ ist.)

n_1 *ist also die Anzahl der* P, *für welche die Zahlen in* (10) *alle gleich* 1 *sind.*

9. Ich wiederhole auch hier die *Definition der D-Zerfällungen zweiter Art*:

Es sei auch $D_i (i = 1, 2)$ Diskriminante eines quadratischen Zahlkörpers oder gleich 1. Ist $D_1 D_2 = D$, so nenne ich das Zahlenpaar D_1, D_2 eine D-Zerfällung; D_1, D_2 und D_2, D_1 sind als nicht verschiedene D-Zerfällungen zu betrachten. Ist überdies

$$\left(\frac{D_1}{q_2}\right) = 1\,, \quad \left(\frac{D_2}{q_1}\right) = 1\,,$$

wobei $q_i (i = 1, 2)$ alle rationalen Primteiler von D_i bedeutet, so spreche ich von einer D-Zerfällung zweiter Art.

Dann gilt der

Satz. 2^{e_4} *ist gleich der Anzahl der verschiedenen D-Zerfällungen zweiter Art.*

Für die Richtigkeit des Satzes reicht es aus, folgendes zu bemerken: Die *verschiedenen* D-Zerfällungen entstehen aus *allen* z. B. durch die Einschränkung $p_t \mid D_1$; diese D_1 stimmen dann mit den P in (10) überein; endlich ist ersichtlich, daß („die Menge der zu P gehörigen Spalten von M_D ist eine Einheitsmenge" d. h.) „die Zahlen in (10) sind alle gleich 1" und „$P, \frac{D}{P}$ $(= P'$ oder $4P')$ ist eine D-Zerfällung zweiter Art" gleichwertige Aussagen sind [12]).

10. *Anmerkung.* Wir haben gesehen, daß e_4 eine Eigenschaft der Matrix M_D ist, die sich auf zweierlei Weise äußert. Und zwar ist e_4 eine Eigenschaft der Zeilen allein und auch eine der Spalten allein. Um dies noch deutlicher auszudrücken, definiere ich die Gruppe der Mengen $a, b, \ldots$ von Zeilen einer Matrix mit der Kompositionsregel: ab enthält die und nur die Zeilen, welche aus den Mengen a, b in einer und nur in einer enthalten sind. Die Gruppe ist abelsch vom Typus $(2, 2, \ldots, 2)$; das Einheitselement ist die leere Menge. Eine Untergruppe davon bilden die Einheitsmengen von Zeilen. Alles ist auch für die Mengen von Spalten zu verstehen. Dann gelten:

a. e_4 *ist die Anzahl der unabhängigen Elemente in der Gruppe der Einheitsmengen von Spalten in* M_D;

b. e_4 *ist um* 1 *weniger als die Anzahl der unabhängigen Elemente in der Gruppe der Einheitsmengen von Zeilen in* M_D [13]).

Dabei ist „unabhängig" in dem gewöhnlichen gruppentheoretischen Sinne zu verstehen.

---

[12]) Bezüglich der Gruppe der D-Zerfällungen usw. weise ich auf die Arbeiten[2]) hin.

[13]) Leicht ersichtlich führt: **a.** zur (aus RR) bekannten Fassung des Satzes, **b.** zur Fassung des Satzes, wie am Anfang von[9]). Es ist eine merkwürdige Erscheinung, daß beide Eigenschaften von M_D (nach Spalten bzw. nach Zeilen) sich ohne jeden Zwang durch die Klassenkörpertheorie bzw. mit Hilfe nur arithmetischer Mittel ergeben, während die Äquivalenz beider der Hilfssatz in **7.** klarstellt.

Eingegangen 12. September 1933.

Eine obere Schranke der Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*).

Von *L. Rédei* in Mezötur (Ungarn).

Ich werde hier aus meinem Satze [1]) über die Anzahl e_4 der durch vier teilbaren Invarianten der absoluten Klassengruppe eines beliebigen quadratischen Zahlkörpers k eine obere Schranke für e_4 bestimmen.

Ich nenne eine Fundamentaldiskriminante eine solche ganze rationale Zahl, die auch die Diskriminante eines quadratischen Zahlkörpers ist, und die nur einen einzigen rationalen Primteiler hat; diese sind also -4, 8, -8 und die (positiven oder negativen) Primzahlen der Gestalt $4m+1$. Offenbar läßt sich die Diskriminante D von k in der Form $D = d_1 d_2 \cdots d_t$ darstellen, wobei die Faktoren d_i paarweise relativ prime Fundamentaldiskriminanten sind, die, von der Reihenfolge abgesehen, eindeutig durch k bestimmt sind. Davon sei r_1 bzw. $2r_2 - v$ die Anzahl der positiven bzw. negativen, wobei r_1, r_2 nicht negative ganze Zahlen sind, und $v = 0$ oder 1. Es ist t die Anzahl der verschiedenen rationalen Primfaktoren von D und es besteht

$$t = r_1 + 2r_2 - v. \tag{1}$$

Ich setze

$$r = r_1 + r_2 - 1. \tag{2}$$

Satz. *Es ist*

$$e_4 \leqq r_1 + r_2 - 1 (= r). \tag{3}$$

Damit ist für e_4 eine echte obere Schranke gegeben, in dem Sinne, daß es für jedes System r_1, r_2, $v (r_1 + 2r_2 - v \geqq 1)$ unendlich viele solche k gibt, für welche in (3) „$=$“ *besteht* [2]).

*) Die vorliegende Arbeit wird auch ungarisch erscheinen im Math. u. Naturwiss. Anz. d. ung. Ak.

[1]) L. Rédei u. H. Reichardt: Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, dieses Journal **170** (1933), S. 69—74.

[2]) Bemerkungen zum Satz: Sind alle zu D gehörigen Fundamentaldiskriminanten positiv, oder gibt es darunter eine einzige, die negativ ist, so ist die rechte Seite von (3) gleich $t-1$, der Anzahl e_2 der geraden Invarianten; in jedem anderen Falle ist diese rechte Seite kleiner als e_2 (ich hatte dies schon in der Arbeit [1]) bemerkt). Bei einem gegebenen t scheint ein „großes“ r_2 eine kleine Anzahl der durch 4 teilbaren Invarianten und somit auch der Idealklassen nach sich zu ziehen. Im ungünstigsten Falle $r_1 = 0$, $t = 2r_2$ $(v = 0,\ D > 0)$ ist $e_4 \leqq \frac{t}{2} - 1 = \frac{e_2 - 1}{2}$. Man sieht sofort die Analogie mit dem Dirichletschen Satze über die Anzahl der unabhängigen Grundeinheiten in einem beliebigen Zahlkörper. Diese Analogie wird noch dadurch verstärkt, daß den positiven und negativen Fundamentaldiskriminanten reelle bzw. imaginäre quadratische Körper entsprechen, und daß auch e_4 die Anzahl unabhängiger Basiselemente einer (zwar endlichen) Gruppe bedeutet. Doch wird diese Analogie dadurch eingeschränkt, daß die jetzt erwähnten Körper nicht konjugiert sind, ihre Anzahl nicht r_1, $2r_2$ (sondern r_1, $2r_2 - v$) ist, endlich $r_1 + r_2 - 1$ keine genaue Anzahl für e_4 ist, sondern nur eine (echte) obere Schranke.

Es bedeute (G) die Ordnung der Gruppe G. Für reelle Werte sei $[x]$ die ganze rationale Zahl mit $x-1<[x]\leqq x$. Ich beweise erst den

Hilfssatz. Ist $a_1, a_2, \ldots, a_n$ eine unabhängige Basis der abelschen Gruppe G von der Ordnung $(G)=2^n$, und ist H eine Untergruppe von G, die die Eigenschaft

A. „*Die Anzahl der in je zwei Elementen von H enthaltenen gemeinsamen Faktoren* [3]) *ist stets eine gerade Zahl*"

besitzt, so ist

$$(H)\leqq 2^{\left[\frac{n}{2}\right]}. \quad (4)$$ [4])

Leicht ersichtlich hat bei einem geraden n mit H zusammen auch $H_1=\{H, a_1a_2\cdots a_n\}$ die Eigenschaft A. Vor allem gilt also die folgende Bemerkung: Besteht der Hilfssatz für ein bestimmtes n, und gilt für ein H das „$=$" in (4), so enthält H das Element $a_1a_2\cdots a_n$.

Der Hilfssatz ist richtig für $H=1$ (Einheitselement in G) und somit auch für $n=1$. Ich setze den Hilfssatz für Anzahlen $<n$ voraus, indem ich zugleich $n\geqq 2$, $H\neq 1$ annehme.

Nach geeigneter Bezeichnung hat H ein solches Element a, das den Faktor a_n enthält. Dann ist $H=H'\cdot\{a\}$, wobei H' eine Untergruppe von $G'=\{a_1, a_2, \ldots, a_{n-1}\}$ ist. Offenbar bestehen auch für das Paar G', H' (statt G, H) die Prämissen des Hilfssatzes (dabei ist selbstverständlich $a_1, a_2, \ldots, a_{n-1}$ als Basis für G' zu nehmen). Nach der Voraussetzung ist also

$$(H')\leqq 2^{\left[\frac{n-1}{2}\right]}. \quad (5)$$

Dabei gilt noch $(H)=2(H')$. Daraus folgt sofort (4), wenn n gerade ist, da dann $\left[\frac{n}{2}\right]=\left[\frac{n-1}{2}\right]+1$, und auch wenn in (5) „$<$" gilt. Es bleibt also nur der Fall übrig, im welchem n ungerade und

$$(H')=2^{\left[\frac{n-1}{2}\right]}$$

ist. Dann läßt sich also auf H' die vorige Bemerkung anwenden ($n-1$ ist gerade!) und somit muß H' das Element $a_0=a_1a_2\cdots a_{n-1}$ enthalten. Hiernach sind a und a_0 Elemente von H. Da aber die gemeinsamen Faktoren von a und a_0 alle und nur die Faktoren von aa_n^{-1} sind, und deren Anzahl eine ungerade Zahl ist, so haben wir einen Widerspruch mit A. erhalten. Damit ist der Hilfssatz bewiesen.

Nunmehr sei G die Gruppe *aller* D-Zerfällungen D_1, D_2, [5]) wobei also D_1 und D_2 alle Teiler von $D=d_1d_2\ldots d_t$ sind, die die Gestalt $d_gd_h\cdots d_m$ haben, und dabei soll immer $D_1D_2=D$ bestehen; $D_i (i=1, 2)$ ist also Diskriminantenzahl oder 1. Es sind D_1, D_2 die Glieder der D-Zerfällung, D_i das i-te Glied. (Ich hatte in der Arbeit [1]) die D-Zerfällungen,

---

[3]) Da G vom Typus $(2, 2, \ldots, 2)$ ist, so läßt sich jedes Element a von G in der Gestalt $a_ga_h\cdots a_m$ annehmen, wobei $a_g, a_h, \ldots, a_m$ verschieden, und von der Reihenfolge abgesehen eindeutig bestimmt sind; ich nenne sie die „Faktoren" von a. — Es ist A. auch auf je zwei gleiche Elemente von H zu beziehen; der Eigenschaft A. zufolge ist also jedes Element von H das Produkt von Faktoren in gerader Anzahl. — Selbstverständlich kann H die Eigenschaft A. verlieren, wenn man zu einer anderen Basis übergeht.

[4]) Beispiele für den Extremfall in (4): 1. $n=8$; $H=\{a_1a_2, a_3a_4, a_5a_6, a_7a_8\}$ und $H=\{a_1a_2a_3a_4, a_3a_4a_5a_6, a_1a_3a_5a_7, a_2a_4a_6a_8\}$; 2. aus den vorigen stellen sich Beispiele mit $n=7$ heraus, wenn man das vierte Element aus den Klammern { } wegschafft.

[5]) Die Gruppe der D-Zerfällungen aus der Arbeit [1]) (S. 73) gebe ich hier in etwas verändertem Sinn wieder.

die voneinander nur in der Reihenfolge der Glieder abweichen, als „nicht verschieden" definiert. Die Anzahl der letzteren ist halb so groß, wie die der Elemente von G.) Die aus D_1, D_2 und E_1, E_2 zusammengesetzte D-Zerfällung soll die sein, die aus dem Zahlenpaar D_1E_1, D_2E_1 nach dem Wegschaffen sämtlicher Faktoren d_i^2 entsteht. Nach dieser Zusammensetzungsregel bildet G ersichtlich eine abelsche Gruppe vom Typus $(2, 2, \ldots, 2)$ und von der Ordnung 2^t; das Einheitselement ist 1, D. Da die D-Zerfällung D_1, D_2 schon durch ihr erstes Glied bestimmt ist, bezeichne ich sie mit $D_1, \ldots$; natürlich ist diese verkürzte Bezeichnung nur so lange möglich, wie D ungeändert bleibt. Es ist $G = \{\Delta_1, \Delta_2, \ldots, \Delta_t\}$, wobei $\Delta_i = d_i, \ldots$ $(i = 1, 2, \ldots, t)$ eine Basis für G ist.

Es bedeute G_2 die Untergruppe von G, bestehend aus denjenigen D-Zerfällungen 2. Art (s. Arbeit [1]), S. 70), die ein positives erstes Glied haben.

Es seien $\Delta = P_1P_2, \ldots$; $\Delta' = P_1P_3, \ldots$ solche Elemente von G_2, in denen P_2, P_3 relativ prim sind und $P_i \neq 1 (i = 1, 2, 3)$. Dann ist auch $\Delta'' = \Delta\Delta' = P_2P_3, \ldots$ in G_2. Aus der Definition der D-Zerfällungen 2. Art folgt

$$(6) \qquad \left(\frac{P_1P_2}{P_3}\right) = 1, \quad \left(\frac{P_1P_3}{P_2}\right) = 1, \quad \left(\frac{P_2P_3}{P_1}\right) = 1.$$

Es ist der „Umkehrfaktor" $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)$ für teilerfremde Diskriminantenzahlen a, b gleich -1 oder 1, je nachdem a, b beide negativ sind oder nicht. Da die Zahlen $P_i (i = 1, 2, 3)$ das gleiche Vorzeichen haben, folgt aus (6) durch Multiplikation, daß P_1 positiv ist (ähnliches gilt natürlich auch für P_2 und P_3). Nun gilt dies auch dann, wenn man $P_i \neq 1$ nicht voraussetzt.

Ich nenne das Basiselement $\Delta_i = d_i, \ldots$ $(i = 1, 2, \ldots, t)$ von G „positiv" oder „negativ", je nach dem d_i positiv oder negativ ist. Da die Anzahl der in je einem Element von G_2 enthaltenen „negativen" Faktoren Δ_i eine gerade Zahl ist, folgt daraus und aus dem vorigen:

(7) *Die Anzahl der „negativen" Δ_i, die je zwei Elemente von G_2 als gemeinsame Faktoren enthalten, ist stets eine gerade Zahl.*

Ich wähle nunmehr die Bezeichnungen so, daß $\Delta_1, \Delta_2, \ldots, \Delta_{r_1}$ „positiv" sind, und ich betrachte die Gruppe $G_2' = \{G_2, \Delta_1, \Delta_2, \ldots, \Delta_{r_1}\}$. Offenbar besteht dann (7) auch für G_2' statt G_2.

Ich setze noch $G' = \{\Delta_1, \Delta_2, \ldots, \Delta_{r_1}\}$, $G'' = \{\Delta_{r_1+1}, \ldots, \Delta_t\}$. Dann ist $G = G' \times G''$ (direktes Produkt!), weiter ist $G'_2 = G' \times H$, wobei $H < G''$. Leicht ersichtlich besteht (7) auch für H, und somit befriedigt das Paar G'', H die Prämissen des Hilfssatzes. Es ist also

$$(H) \leqq 2^{\left[\frac{t-r_1}{2}\right]} = 2^{\left[\frac{2r_2-v}{2}\right]} = 2^{r_2-v},$$

d. h.

$$(8) \qquad (G_2) \leqq (G_2') = (G') \cdot (H) \leqq 2^{r_1+r_2-v}.$$

Ist *erstens* $D < 0$, so hat jede D-Zerfällung ein positives (erstes oder zweites) Glied, und somit sind die *verschiedenen* (nämlich im Sinne der Arbeit [1]), S. 70) D-Zerfällungen 2. Art alle und nur die Elemente von G_2. Da nun $v = 1$, so ist also nach (8) die Anzahl der verschiedenen D-Zerfällungen 2. Art höchstens gleich

$$2^{r_1+r_2-1}.$$

Ist *zweitens* $D > 0$, so besteht nach der Arbeit [1]), S. 71, Anm. [14]) jede D-Zerfällung 2. Art aus 2 positiven Gliedern, und somit ist die Anzahl der *verschiedenen* D-Zerfällungen

2. Art halb so groß wie die der Elemente von G_2. Da nun $v = 0$, so ergibt sich aus (8) ein ähnliches Resultat wie vorher.

Daraus folgt (3) nach dem Satze aus der Arbeit [1]), S. 73.

Ich gebe noch (unendlich viele) Beispiele für das „ $=$ “ in (3) an. Ich bestimme dazu verschiedene ungerade Primzahlen $p_1, p_2, \ldots, p_{r_1} (> 0)$; $p_{r_1+1}, \ldots, p_t (< 0)$ der Gestalt $4m + 1$, mit

$$\left(\frac{p_j}{p_i}\right) = 1 \qquad (1 \leqq i < j \leqq t).$$

Dann hat $D = p_1 p_2 \cdots p_t$ die gewünschte Eigenschaft. Bezeichnet man nämlich die Zahlen $p_1, p_2, \ldots, p_{r_1}$; $p_{r_1+1}\, p_{r_1+2}, p_{r_1+3}\, p_{r_1+4}, \ldots$ (das letzte Glied ist $p_{t-1}\, p_t$ oder p_t, je nachdem $v = 0$ oder 1 ist) der Reihe nach mit $\Delta_1, \Delta_2, \ldots, \Delta_{r+1}$, so ist D das Produkt der letzteren, und leicht ersichtlich sind $\Delta_i, \frac{D}{\Delta_i} (i = 1, 2, \ldots, r)$ unabhängige D-Zerfällungen 2. Art. Nach dem eben erwähnten Satze aus der Arbeit [1]) und nach dem schon bewiesenen (3) ist $e_4 = r$. Damit ist der vorliegende Satz in allen Teilen bewiesen [6]).

[6]) Ähnlich lassen sich Beispiele konstruieren mit geradem D. — Außer den oben gegebenen gibt es noch ungerade Diskriminanten, für die in (3) „ $=$ “ besteht. Dazu sind Gruppen wie in [4]) zu konstruieren, und jede gibt Anlaß zur Konstruktion einer unendlichen Anzahl der gewünschten D.

Eingegangen 12. September 1933.